

EXHIBIT 1

Trials@uspto.gov
571-272-7822

Paper: 10
Entered: Nov. 17, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

BT AMERICAS INC.,
Patent Owner.

IPR2023-00889
Patent 7,895,641 B2

Before KARL D. EASTHOM, GEORGIANNA W. BRADEN, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

EASTHOM, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

IPR2023-00889

Patent 7,895,641 B2

I. INTRODUCTION

Palo Alto Networks, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–25 (the “challenged claims”) of U.S. Patent No. 7,895,641 B2 (Ex. 1001, “the ’641 patent”). Paper 2 (“Pet.”). BT Americas Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). With our permission (Ex. 3001), to address claim construction issues, Petitioner filed a Reply (Paper 7, “Reply”), and Patent Owner filed a Sur-reply (Paper 8, “Sur-reply”).

We have authority to determine whether to institute an *inter partes* review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4. Institution of an *inter partes* review requires that “the information presented in the petition and . . . any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a).

For the reasons set forth below, we determine that there is a reasonable likelihood that Petitioner will prevail with respect to at least one challenged claim. Accordingly, we institute an *inter partes* review of the ’612 patent.

II. BACKGROUND

A. *Real Parties in Interest*

Petitioner identifies itself as the real party in interest. Pet. 2. Patent Owner identifies itself and British Telecommunications PLC as real parties in interest. Paper 4, 1.

B. *Related Proceedings*

The parties identify the following district court cases involving the ’641 patent: *British Telecommunications PLC v. Fortinet, Inc.*, 1:18-cv-01018-CFC-MPT (D. Del.) and *British Telecommunications PLC and BT*

IPR2023-00889

Patent 7,895,641 B2

Americas, Inc. v. Palo Alto Networks, Inc., 1:22-cv-01538 (D. Del.). Pet. 3; Paper 4, 1. The parties also collectively identify as related matters the following *inter partes* review proceedings: IPR2023-00888 (denying institution with respect to U.S. Patent No. 7,159,237 B2); IPR2019-01325 (denying institution with respect to U.S. the '641 patent); and, IPR2019-01325 (denying institution with respect to U.S. Patent No. 7,159,237 B2). Pet. 3; Paper 4, 1.

C. The '641 Patent (Ex. 1001)

The '641 patent, "Method and System for Dynamic Network Intrusion Monitoring, Detection and Response," issued on February 22, 2011 with a possible effective filing date of March 16, 2000 (based on a continuation of a patent and a provisional application). Ex. 1001, codes (45), (54), (60), (63). The '641 patent relates to dynamic network intrusion monitoring, detection, and response. Ex. 1001, 1:18–20. The '641 patent discloses that system administrators normally do not have time, ability, or resources to monitor large amounts of constantly-updated audit information, hacking activities, and new attack tactics, tools, and trends. *Id.* at 1:36–41. According to the '641 patent, such limitations point to a need for automatic defenses. *Id.* at 1:44–50. Prior art automatic defenses are at a disadvantage against an intelligent attack. *Id.* at 1:51–53.

To address intelligent attacks, the '641 patent discloses deploying and providing a managed security monitoring service ("MSM service") that monitors a customer's network activity using a probe or sentry system. Ex. 1001, 1:59–63. The MSM service first collects status data from monitored components. *Id.* at 1:63. The MSM service then filters or analyzes the collected data for activity that potentially implicates security concerns. *Id.* at 1:63–65. The MSM service further alerts and transmits information about

IPR2023-00889

Patent 7,895,641 B2

such activity to trained security analysts working at secure operation centers (“SOCs”). *Id.* at 1:65–67. The MSM service guides the security analysts and customer through an appropriate response and optionally, follow-up. *Id.* at 1:67–2:2. The MSM service may accommodate network-specific needs and provide feedback. *Id.* at 2:32–35.

Figure 1 of the ’641 patent follows:

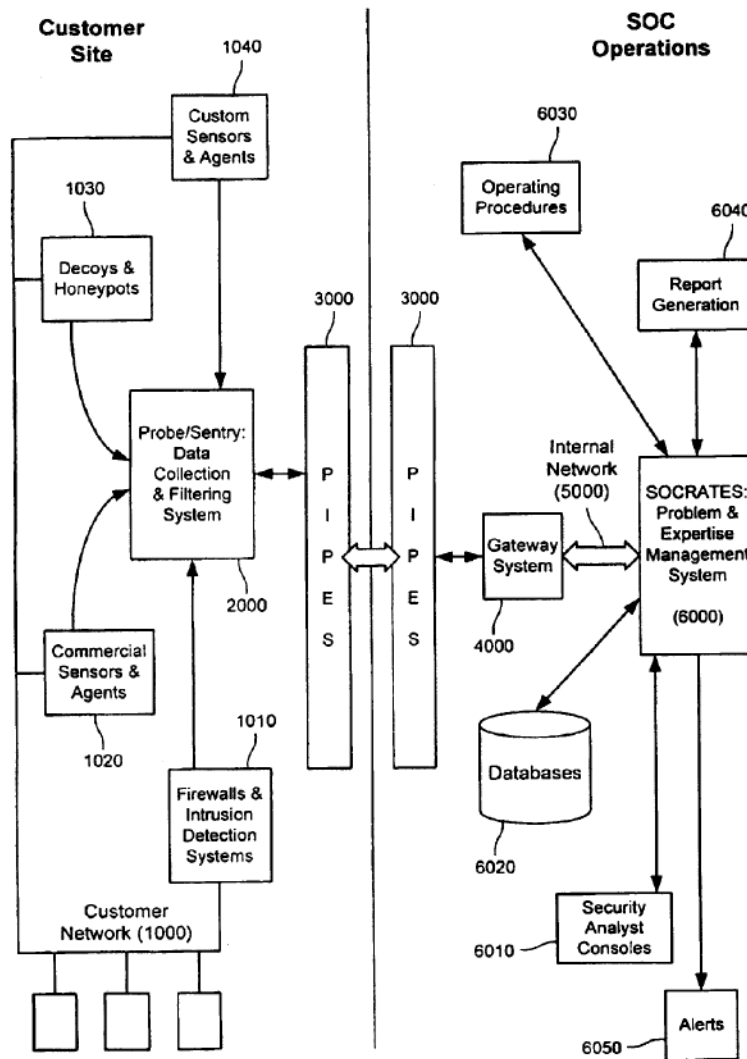


FIG. 1

Figure 1 depicts “an overview of the system architecture of an exemplary embodiment.” *Id.* at 3:66–67. Figure 1 illustrates components and systems that operate on the customer site (within the customer’s firewall, on the left),

IPR2023-00889

Patent 7,895,641 B2

and components and systems that operate within the SOC (within the SOC firewall, on the right). *Id.* at 4:45–49. Pipes 3000 provides an encrypted, secure communications path and message protocol for messages sent back and forth between probe/sentry system 2000 at the customer site and gateway system 4000 at the SOC. *Id.* at 5:50–54.

Figure 2 of the '641 patent is reproduced below:

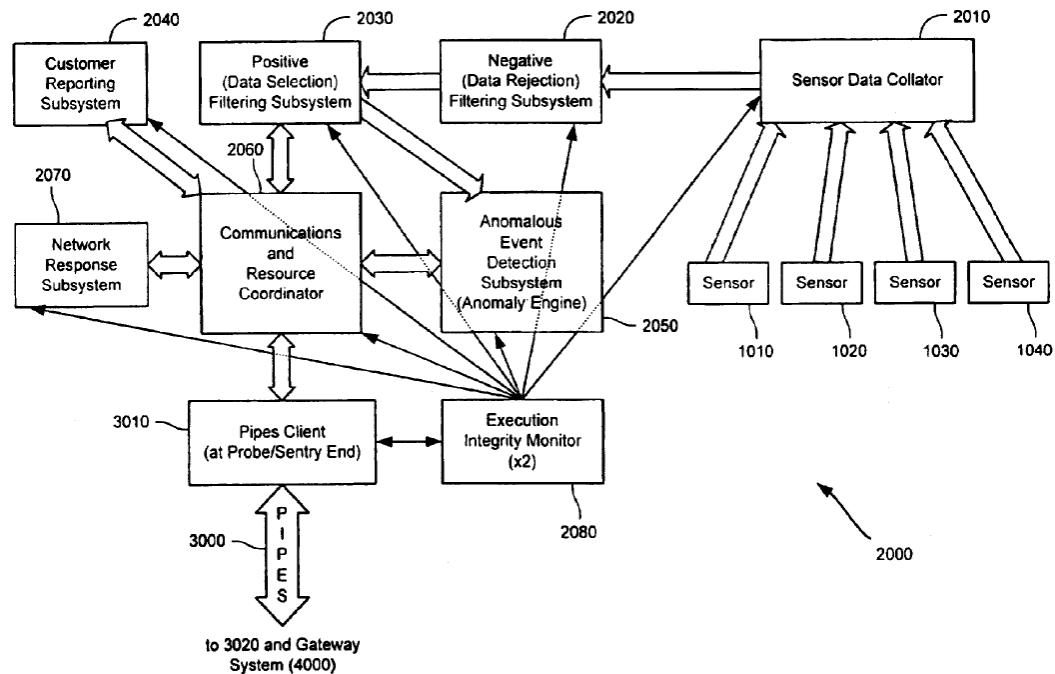


FIG. 2

Figure 2 depicts “a system overview of an exemplary embodiment of a probe/sentry system.” Ex. 1001, 4:1–3. Sensors 1010, 1020, 1030, and 1040 collect status data first filtered by negative filtering subsystem 2020, which discards uninteresting information, and then filtered by positive filtering subsystem 2030, which selects potentially interesting information that it forwards to communications and resource coordinator 2060. Ex. 1001, 8:51–55. Status data that negative filtering subsystem 2020 does not discard and that positive filtering subsystem 2030 does not allow constitutes “residue” that flows to anomaly engine 2050 for further analysis. *Id.* at

IPR2023-00889

Patent 7,895,641 B2

8:55–59. Anomaly engine 2050 determines which residue information may be worthy of additional analysis and sends that residue information to communications and resource coordinator 2060 for forwarding to the SOC.

Id. at 8:59–62. “Communications and resource coordinator 2060 creates sentry messages out of the interesting status data and forwards those messages on to gateway system 4000 via Pipes 3000.” *Id.* at 8:66–9:2.

As part of an SOC, the ’641 patent further discloses a Secure Operations Center Responsive Analyst Technical Expertise System (“SOCRATES”) for generating “event records” and “problem tickets” for customers experiencing potential security issues that security analysts handle. Ex. 1001, 3:61, 10:11–23. Specifically, “[t]he SOCRATES system is a consolidated system used to manage customers’ problems and the supporting data helpful in resolving such problems.” *Id.* at 9:56–58. The SOCRATES system “provides security analysts at a SOC a single, integrated system with which to track information concerning, for example, problems, companies, people, contacts, tools, and installed network components and known vulnerabilities.” *Id.* at 9:58–62.

IPR2023-00889

Patent 7,895,641 B2

Figure 4 of the '641 patent follows:

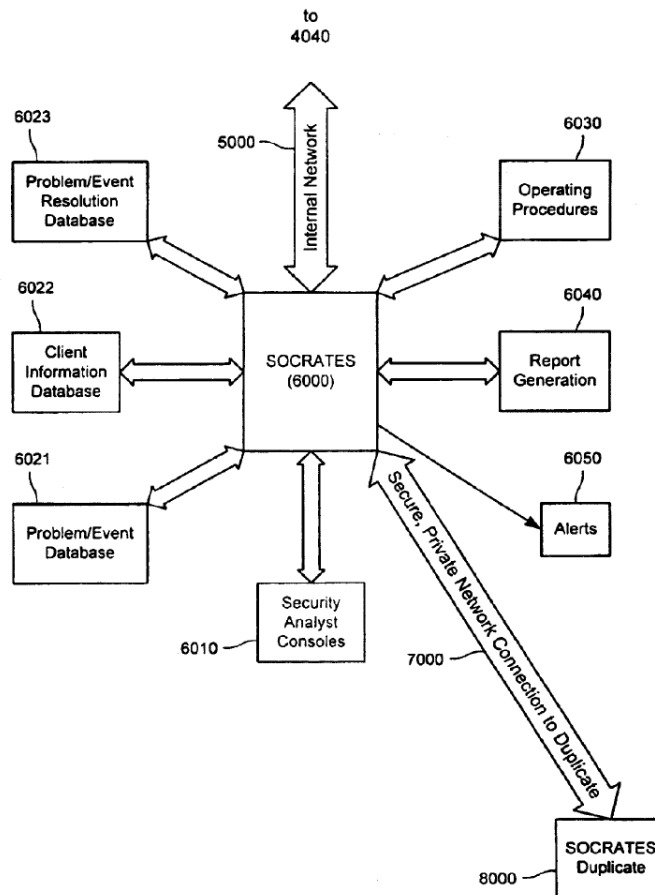


FIG. 4

Figure 4 depicts “a system overview of an exemplary embodiment of a ‘SOCRATES’ problem and expertise management system.” *Id.* at 9:54–56. In relation to Figure 4, “[g]ateway messages arrive at SOCRATES 6000 from gateway system 4000 via internal network 5000” and “SOCRATES 6000 first creates from these gateway messages ‘event records,’ which can be stored in problem/event database 6021.” *Id.* at 10:11–16. “Event records may then be linked with other event records stored in problem/event database 6021 and with information from a variety of databases (including customer information from client information database 6022 and problem resolution information from problem/event resolution database 6023) to

IPR2023-00889

Patent 7,895,641 B2

form ‘problem tickets.’” *Id.* at 10:16–22. The problem tickets “are then opened and displayed on security analyst consoles 6010 to security analysts for handling.” *Id.* at 10:22–23.

D. Illustrative Claims 1 and 18

As noted previously, Petitioner challenges claims 1–25 of the ’641 patent, of which claims 1 and 18 are independent. Pet. 1; Ex. 1001, 33:25–34:63. Claims 1 and 18 are illustrative of the challenged subject matter and follow:

1. A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:
 - a) a sensor coupled to collect status data from at least one monitored component of the network;
 - b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
 - c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
 - d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
 - e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

18. A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:

creating an event record for information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering;

IPR2023-00889

Patent 7,895,641 B2

correlating the event record with customer information and a symptom record;

using the correlated symptom record to link the event record to problem resolution information;

consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket; and

providing the problem ticket to a security analyst console for analysis.

E. Asserted Challenges to Patentability and Evidence of Record

Petitioner challenges the patentability of claims 1–25 of the ’641 patent based on the following references:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–7, 15–17	103 ¹	Duvall ² , Chu ³
7–13, 16	103	Duvall, Chu, Trcka ⁴
14, 15	103	Duvall, Chu, Trcka, Ziese ⁵
18–25	103	Duvall, Chu, Cogger ⁶

In support of its patentability challenge, Petitioner relies on the Declaration of Kevin Jeffay, Ph.D. (“Dr. Jeffay”). Ex. 1003. In support of its Preliminary Response, Patent Owner relies on the Declaration of Wenke

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”) revised 35 U.S.C. § 103 (effective March 16, 2013). The ’237 patent’s filing date precedes March 16, 2013. Ex. 1001, code (22). Accordingly, for purposes of institution, the pre-AIA version of 35 U.S.C. § 103 applies.

² US Patent 5,884,033, issued Mar. 16, 1999, filed May 15, 1996. Ex. 1004.

³ Yang-hua Chu, *Trust Management for the World Wide Web*, M.I.T. (June 13, 1997). Ex. 1005.

⁴ US Patent Application Publication No. 2001/0039579 A1, published Nov. 8, 2001, filed May 7, 1997. Ex. 1014.

⁵ US Patent 6,484,315 B1, issued Nov. 19, 2002, filed Feb. 1, 1999. Ex. 1015.

⁶ US Patent 6,859,783 B2, issued Feb. 22, 2005, filed Sep. 24, 1998. Ex. 1033.

IPR2023-00889

Patent 7,895,641 B2

Lee, Ph.D. (Ex. 2001) and the Declaration of Bruce Schneier (Ex. 2002), a named inventor of the '237 patent.

F. Claim Construction

A claim “shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b).” 37 C.F.R. § 42.100(b). Under that standard, the “words of a claim ‘are generally given their ordinary and customary meaning.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).

Petitioner asserts that “no claim terms require an explicit construction” and that “the challenged claims are unpatentable under either the ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention in light of the specification and the prosecution history, or the district court’s previous claim constructions. Pet. 12–13 (citing Ex. 1012 (district court claim construction); Ex. 1013 (same)).

Patent Owner asserts that Petitioner misconstrues “post-filtering residue.” Prelim. Resp. 32–35. Claim 1’s limitation 1.b recites “a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.” Independent claim 18 recites a similar limitation. *Supra* § II.D.

Patent Owner argues that “post-filtering residue” precludes further filtering, because “the residue produced after filtering is complete.” *Id.* at 33. Patent Owner concedes that the “post-filtering residue” requires further “analysis that follows the [initial] filtering” according to the claim language

IPR2023-00889

Patent 7,895,641 B2

and according to the '641 patent specification. *See id.* at 33–34 (citing Ex. 1001, 9:55–62). According to Patent Owner, Petitioner's implicit construction of the limitation suggest “that the ‘plain language of this element does not require any data to actually be ‘discarded’ or ‘selected by filtering’—only that the ‘post-filtering residue is data neither discarded nor selected by filtering.’” *Id.* at 30. Patent Owner contends Petitioner omits the requirement that the “‘residue’ be ‘post-filtering’ and impermissibly broadens the residue to include any data—not just status data.” *Id.* at 33.⁷

The '641 patent specification and claim language do not support Patent Owner. Limitation 1.b refers to “post-filtering” residue in relation to filtering that occurs prior to arriving at the residue, it does not preclude further filtering of the residue. The '641 patent specification supports this plain meaning on this preliminary record with respect to precluding filtering of residue, as Petitioner argues. Reply 1–2 (citing Ex. 1001, 8:51–62). At the cited passage, the '641 patent specification describes “additional analysis” of “residue information,” and implies that “data discrimination analysis,” which includes “filtering,” is part of such “additional analysis”:

Anomaly engine 2050 determines what residue information may be worthy of additional analysis and sends such information to communications and resource coordinator 2060 for forwarding to the SOC. *Negative filtering, positive filtering, and residue analysis are examples of data discrimination analyses, other types of which are well-known to those skilled in the art.*

Ex. 1001, 8:59–65 (emphasis added).

⁷ As discussed below, Patent Owner admits that IP addresses are status data, but argues that “Petitioner bears the burden to show how Duvall actually analyzes any leftover status data to identify potentially security related events.” Prelim. Resp. 35.

IPR2023-00889

Patent 7,895,641 B2

On the other hand, like Petitioner, we generally agree with Patent Owner that limitation 1.b requires a filtering process that produces the claimed residue with the filtering followed by an analysis of the post-filtering residue. *See* Reply 2 (citing Prelim. Resp. 33). We also agree that claim 1 requires filtering and analysis of status data. Nonetheless, as discussed in detail below, we find Duvall teaches the disputed limitation even under Patent Owner's construction.

We only explicitly construe claim terms "that are in controversy, and only to the extent necessary to resolve the controversy." *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Consequently, we need not explicitly construe any other terms and rely on the plain and ordinary meaning of such other claim terms for purposes of institution.

G. Principles of Law Regarding Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The obviousness question requires resolving underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-

IPR2023-00889

Patent 7,895,641 B2

obviousness.⁸ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Determining “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue” also helps to resolve the obviousness question. *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result also may weigh in the ultimate determination of obviousness. *See id.* at 416–417.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b). The burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

H. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation marks omitted). Furthermore, the prior art itself can reflect the appropriate level of ordinary skill in the art. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

⁸ Patent Owner contends that it “previously raised secondary considerations in response to a prior petition against the ’641 Patent” that “apply equally here,” and “Petitioner failed to address any of these secondary considerations.” Prelim. Resp. 12. Patent Owner fails to provide a citation to this “prior petition,” fails to allege a nexus to the claimed invention, and fails to show clearly what type of secondary considerations are at issue. *See id.* at 12–13 (citing Ex. 2001 ¶¶ 72–74).

IPR2023-00889

Patent 7,895,641 B2

Here, Petitioner asserts a person of ordinary skill in the art at the time of the '641 patent, “would have had a B.S. degree in Computer Science, Computer Engineering, or an equivalent field, as well as at least 2–3 years of academic or industry experience in the design, analysis, and monitoring of computer networks, including issues of network security and network administration, or comparable industry experience.” Pet. 11 (citing Ex. 1003 ¶¶ 63–64). Patent Owner does not dispute Petitioner’s proposed level of skill. Prelim. Resp. 31.

For the purposes of this Decision, we adopt Petitioner’s level of ordinary skill in the art, because it is consistent with the '641 patent and the prior art of record, except that we delete the qualifier “at least” in the phrase “at least 2–3 years” to eliminate vagueness as to the stated amount of academic or industry experience.

I. Overview of Asserted Prior Art of Record

1. Duvall (Ex. 1004)

Duvall is a U.S. Patent titled “Internet Filtering System for Filtering Data Transferred over the Internet Utilizing Immediate and Deferred Filtering Actions.” Ex. 1004, codes (10), (54). Duvall relates to “filtering messages transmitted between the Internet and a client computer.” *Id.* at 1:7–8. Duvall discloses a client-based filtering system compares portions of incoming and/or outgoing messages with filtering information stored in a filter database. and determines whether to block or allow the incoming and/or outgoing transmissions of messages in response to the comparison. *Id.* at 1:31–35. Duvall explains that in response to a match between certain information in portions of the message and the filtering information, the system can employ one of a number of different specified blocking options,

IPR2023-00889

Patent 7,895,641 B2

including discarding incoming data, preventing execution of an open command, or replacing parts of received data. *Id.* at 1:35–40.

One embodiment of Duvall, as shown in Figure 1, follows:

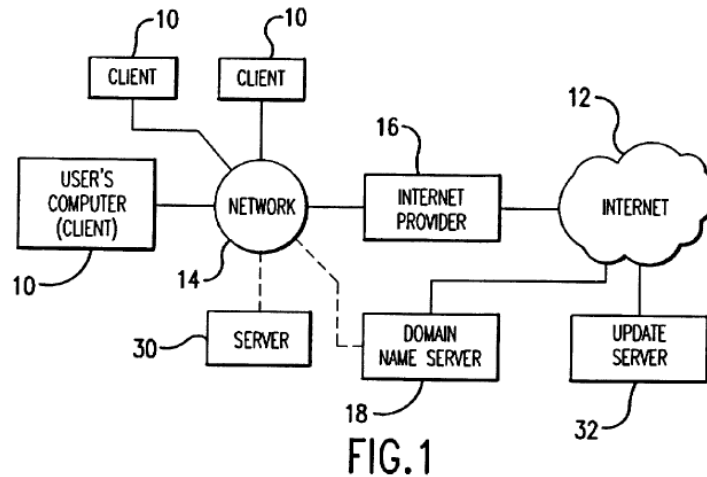


Figure 1 depicts “a block diagram of a network with a client computer for accessing the Internet.” *Id.* at 2:24–25. The network includes a user with a computer that serves as client computer 10 that communicates with other computers over Internet 12.” *Id.* at 2:34–35. According to Internet Protocol version 4, each computer on or connected to the Internet has an IP address that identifies the location of the computer. *Id.* at 2:51–53. Duvall’s filter system can filter messages on the basis of IP addresses. *Id.* at 4:5–11, 4:37–39.

IPR2023-00889

Patent 7,895,641 B2

Another embodiment of Duvall as shown in Figure 2, follows:

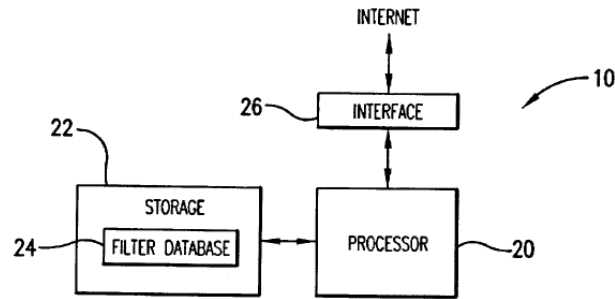


FIG. 2

Figure 2 depicts a block diagram of client computer 10 with a filtering system. *Id.* at 2:26–27. In this embodiment, as shown in Figure 2, “a filtering system resides in client computer 10.” *Id.* at 3:43–44. “Processing by the filtering system is carried out by the computer’s processor 20, and the system uses the computer’s storage 22 to store a filter database 24.” *Id.* at 3:44–46. Duvall also discloses an embodiment in which “the filtering system can be provided from a server 30 that is on the client’s own network 40.” *Id.* at 8:18–21. “This version of the filtering system uses the same type of filter database as a client-based filtering system, but the filter database is located on server 30.” *Id.* at 8:23–26.

Duvall discloses a “filter database [that] has lists of filters, some of which are identified as either ALLOW filters or BLOCK filters for respectively allowing or blocking transmission.” *Id.* at 3:64–66. “Each filter entry in the filter database also has a field for specifying an action to be taken by the client if that filter were retrieved.” *Id.* at 4:12–14. “These actions are essentially divided into two groups, direct action or deferred action.” *Id.* at 4:14–15. “Direct actions indicate that the system should unconditionally allow or unconditionally block the transmission.” *Id.* at 4:15–17. “If . . . it is determined that no immediate action must be taken,

IPR2023-00889

Patent 7,895,641 B2

it is determined whether a deferred action must be taken.” *Id.* at 4:65–67.

Additionally, a filter can indicate that a deferred action should be taken. *Id.* at 4:65–5:1; 6:19–20.

Duvall discloses filters “stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last.” *Id.* at 4:27–29. Duvall further discloses, “[i]f there is no deferred action, the system can default to allow the transmission . . . , or it can default to block the transmission.” *Id.* at 5:1–3. Deferred filter entries preferably have additional fields, including fields for (1) a keyword, typically a command such as GET; (2) a filter pattern to be compared to data in the message, typically a string of characters; (3) a directional indicator (IN/OUT) for indicating incoming or outgoing transmissions; (4) a compare directive for the type of match; and (5) an action to be taken. typically to allow or block the transmission. *Id.* at 5:8–15.

2. *Chu (Ex. 1005)*

Chu is a Master’s thesis titled “Trust Management for the World Wide Web” submitted to the Massachusetts Institute of Technology Department of Electrical Engineering and Computer Science.” Ex. 1005, 3. Chu relates to “trust management . . . in the context of the World Wide Web. Ex. 1005, 3. For example, Chu discloses sample policies addressing the question of “should I download the active content at this URL.” *Id.* at 43–48. Chu discloses policies that employ a “blacklist” and a “whitelist.” *Id.* at 44. The blacklist is a list of sites or directories the computer should not download codes from. *Id.* According to Chu, the use of such lists “can be very effective in practice . . . [because] Firewall vendors can compile a blacklist of Web sites that serve potentially dangerous active codes, and place the list in clients’ firewalls.” *Id.* Chu states that “[t]he blacklist and whitelist ensure

IPR2023-00889

Patent 7,895,641 B2

good automation of the trust decision process if the lists are reasonably complete.” *Id.* If the request URL is neither in the blacklist nor the white list, then Chu discloses that the system can return the term “unknown.”

An example of Chu’s policy and description of its code follows:

Policy in English

Do not download the code if the URL is served from Harvard or CalTech Web servers. Download it automatically if served from MIT. Prompt me for my attention otherwise.

As shown above, Chu directs the system to send the user an attention prompt in that case and states “[u]ser intervention is needed only when the given URL is in neither the blacklist nor the whitelist.” *Id.*

3. *Trcka (Ex. 1014)*

Trcka is a U.S. Patent Application Publication titled “Network Security and Surveillance System.” Ex. 1014, codes (10), (54). Trcka relates to “[a] network security and surveillance system [that] passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic.” *Id.* at code (57). According to Trcka, “[a] set of analysis applications and other software routines allows authorized users to interactively analyze the low-level traffic recordings to evaluate network attacks, internal and external security breaches, network problems, and other types of network events.” *Id.*

Trcka discloses “analysis applications [that] can . . . be used to view, analyze and process . . . traffic data,” including “functionality for performing such actions as displaying user-specified types of network events, conducting pattern searches of selected packet data, reconstructing transaction sequences, and identifying pre-defined network problems.”

Id. ¶ 16. Trcka also discloses “analysis tools . . . for allowing authorized

IPR2023-00889

Patent 7,895,641 B2

users to perform interactive, off-line analyses of recorded traffic data.”

Id. ¶ 53. Trcka discloses a “graphical user interface (GUI)” through which “the user can launch and control the various analysis applications . . .

through a common set of menus and controls.” *Id.* ¶ 79.

4. *Ziese (Ex. 1015)*

Ziese is a U.S. Patent titled “Method and System for Dynamically Distributing Updates in a Network.” Ex. 1015, codes (10), (54).

Ziese discloses “dynamically distributing intrusion detection and other types of updates in a network that substantially eliminate or reduce disadvantages and problems associated with prior methods and systems.”

Id. at 2:2–6. According to Ziese, “programs are automatically updated by downloading and distributing an update in response to an automated event,” and “[a]s a result, systems with a common program separately running at several sites may update each site with no or minimal operator interaction.”

Id. at 2:39–44.

5. *Cogger (Ex. 1033)*

Cogger is a U.S. Patent titled “Integrated Interface for Web Based Customer Care and Trouble Management.” Ex. 1033, codes (10), (54).

Cogger relates to “opening and tracking trouble tickets over the public Internet.” *Id.* at 2:50–52. According to Cogger, “customer profile information is used to prepopulate data fields in dialogs used to open a trouble ticket.” *Id.* at 2:56–57. “Once a trouble ticket is opened, the customer workstation tracks the existing trouble tickets through a browser based graphical user interface.” *Id.* at 2:58–60.

Figure 8(g) of Cogger follows:

IPR2023-00889

Patent 7,895,641 B2

FIG. 8(g)

Figure 8(g) depicts a “graphical user interface[] that may be presented to a customer for opening a new and querying an existing trouble ticket.” *Id.* at 4:49–51. More specifically, Figure 8(g) depicts a “Details” window 283 that includes selectable tabs comprising information about a selected ticket. *Id.* at 20:3–6. According to Cogger, “selection of the ticket tab 287a . . . provides ticket information including: ticket number, ticket product, ticket service, date occurred, trouble description, and organization (ORG) code, etc.” *Id.* at 20:7–10. Further, “[t]he customer tab 287b, circuit tab 287c, and call tab 287d . . . provide additional detailed information including: ticket priority, ticket status, ticket identifier, etc.” *Id.* at 20:10–13. Cogger discloses that “the number of data elements will be different for different types of tickets.” *Id.* at 20:13–15.

IPR2023-00889

Patent 7,895,641 B2

III. ANALYSIS

A. Alleged Obviousness of Claims 1–7 and 15–17 in view of Duvall and Chu

Petitioner contends claims 1–7 and 15–17 would have been obvious to a person of ordinary skill in the art in view of the combined teachings of Duvall and Chu. Pet. 13–49. Patent Owner disputes Petitioner’s contentions with respect to independent claim 1. Prelim. Resp. 35–67.

1. Analysis of Independent Claim 1

i) “A system for operating a probe as part of a security monitoring system for a computer network”

Petitioner contends that “to the extent the preamble is limiting,” Duvall discloses it. Pet. 23. Petitioner reads the preamble onto Duvall’s disclosure of “‘filtering messages transmitted between the Internet and a client computer’ to ensure content that implicates security concerns does not reach recipients.” *Id.* at 24 (quoting Ex. 1004, 1:7–24; citing 1:27–29; Ex. 1003 ¶ 113). According to Petitioner, “Duvall’s filtering system monitors transmissions for questionable content that should be blocked.” *Id.* at 25 (citing Ex. 1004, 3:33–37, 5:8–15, 6:10–42; Ex. 1003 ¶ 119). Petitioner argues that a person of ordinary skill in the art “would have been motivated to block content that may have carried viruses or malware” and that “no modifications would be needed in Duvall’s system—domains (e.g., URLs or IP addresses) believed to carry security-implicating content (e.g., viruses) would simply be included in Duvall’s blocking filters.” *Id.* (citing Ex. 1004, 6:10–27; Ex. 1003 ¶ 115).

Petitioner further contends that Duvall’s server 30 is a probe that provides a filtering system. Pet. 26 (citing Ex. 1004, 1:60–64, 8:18–21, Fig. 1; Ex. 1003 ¶¶ 119–20; Ex. 1013 (district court claim construction), 2).

IPR2023-00889

Patent 7,895,641 B2

According to Petitioner, “Duvall’s server 30 collects and analyzes data from other network components to which it is attached, such as clients 10” and that its “filtering system may be part of a firewall.” *Id.* at 27–28 (citing Ex. 1004, 1:59–64, 8:21–223).

Patent Owner does not challenge Petitioner’s showing regarding the preamble. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

“Whether to treat a preamble term as a claim limitation is determined on the facts of each case in light of the claim as a whole and the invention described in the patent.” *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358 (Fed. Cir. 2010) (internal quotation marks omitted). “Absent clear reliance on the preamble in the prosecution history, or in situations where it is necessary to provide antecedent basis for the body of the claim, the preamble generally is not limiting.” *Symantec Corp. v. Computer Assocs. Int’l, Inc.*, 522 F.3d 1279, 1288 (Fed. Cir. 2008) (internal quotation marks and citation omitted). Additionally, preamble language that merely states the purpose or intended use of an invention generally does not limit the scope of a claim. *See Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp.*, 320 F.3d 1339, 1345 (Fed. Cir. 2003); *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir. 1997). Yet, when the limitations in the body of the claim rely upon or derive essential structure from the preamble, then the preamble acts as a necessary component of the claimed invention and is limiting. *See Eaton Corp. v. Rockwell Int’l Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003).

A “conclusion that some preamble language is limiting does not imply that other preamble language, or the entire preamble, is limiting.” *Cochlear*

IPR2023-00889

Patent 7,895,641 B2

Bone Anchored Sols. AB v. Oticon Med. AB, 958 F.3d 1348, 1355 (Fed. Cir. 2020); see also *TomTom, Inc. v. Adolph*, 790 F.3d 1315, 1322-23 (Fed. Cir. 2015) (holding the court erred in determining that it had to construe the entire preamble if it construed a portion of it) (citing *Loctite Corp. v. Ultraseal Ltd.*, 781 F.2d 861, 868 (Fed. Cir. 1985), *overruled in part on other grounds by Nobelpharma AB v. Implant Innovations, Inc.*, 141 F.3d 1059, 1068 (Fed. Cir. 1998) (en banc in part))). Even when a phrase in a preamble provides a necessary structure for a claim, that preamble structure does not necessarily convert the entire preamble into a limitation, particularly one that only states the intended use of the invention. *Cochlear Bone Anchored*, 958 F.3d at 1355.

Based on the current record, we determine that at least part of the preamble is limiting because limitation 1.e recites “the probe,” referring to “a probe” in the preamble of claim 1 for antecedent basis. Even if the entirety of the preamble is limiting, as discussed below in connection with a discussion of “security-related events,” Petitioner sufficiently shows that Duvall in combination with the teachings of Chu would have rendered obvious the preamble’s “security monitoring system” limitation.

ii) “a) a sensor coupled to collect status data from at least one monitored component of the network”

Petitioner contends that Duvall meets limitation 1.a because Duvall’s server 30 analyzes (i.e., monitors) status data received from clients 10, which reside on the same network. Pet. 26–29. Specifically, Petitioner argues Duvall’s filtering system, which is on a client’s network server 30, **“compares the IP address and/or other information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken.”** *Id.* at 29 (quoting Ex. 1004, 4:22–27, citing

IPR2023-00889

Patent 7,895,641 B2

2:35–37, 2:42–44, Fig. 1). According to Petitioner, the IP address of a message is “status data” because it is data extracted from network traffic and provides information about the status of the network and its component. *Id.* at 30 (citing Ex. 1004, 4:39–42, 5:66–6:27; Ex. 1013, 1). Petitioner also relies on Duvall’s teaching “that information about the data stream can include ‘a particular port and IP address’ with which a client is attempting to communicate, as well as protocol information, URLs, and associated commands (e.g., an HTTP ‘GET command’).” *Id.* at 28 (citing Ex. 1004, 4:39–42, 5:66–6:27).

As noted above, Patent Owner agrees that IP addresses are status data. Prelim. Resp. 33. Patent Owner does not challenge Petitioner’s showing as to limitation 1.a. Prelim. Resp. 31. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the preliminary record and foregoing discussion, we determine that Petitioner sufficiently shows for purposes of institution that Duvall teaches limitation 1.a.

iii) “(b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering”

Petitioner contends that Duvall meets claim limitation 1.b because Duvall discloses filtering based on IP address (i.e., “status data”) and other information: “When a message is transmitted, whether that message is incoming or outgoing with respect to the client computer, the filtering system compares the IP address and/or other information in the data stream

IPR2023-00889

Patent 7,895,641 B2

to the filter entries stored in the database to determine whether some action needs to be taken.” Pet. 29–30 (quoting Ex. 1004, 4:22–27).

Petitioner generally relies on Duvall’s server-based embodiment, which may include the same a filter database as Duvall’s client. *See* Pet. 30 (citing Ex. 1004, Fig. 2, 8:16–26). Regarding the claim limitation “wherein analysis includes filtering followed by an analysis of post-filtering residue,” Petitioner relies on Duvall’s teaching that “[t]he filters are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last,” where the ‘ALLOW’ and ‘BLOCK’ filters are direct action filters.” *Id.* (quoting Ex. 1004, 4:27–30; citing Ex. 1003 ¶¶ 126–27). Analyzing Duvall’s Figure 3, Petitioner explains that for these delayed action filters, “immediate action is not required (i.e., data is neither blocked nor allowed at block 104 (i.e., the data is residue data)),” and “the data is passed for further analysis.” *See id.* at 33–34 (citing Ex. 1004, Fig. 3, 4:50–54). Analyzing Duvall’s Figure 3 further, Petitioner reads the claimed “post-filtering residue is data neither discarded nor selected by filtering” onto Duvall’s “status data that underwent negative and positive filtering,” where Duvall’s data “is neither discarded by such negative filtering nor selected by such positive filtering.” *Id.* (citing Ex. 1003 ¶ 134).

Petitioner further contends that Duvall teaches “identify[ing] potentially security-related events” because “Duvall’s filtering ensures that content implicating security concerns does not reach recipients.” Pet. 35 (citing Ex. 1004, 1:7–24; Ex. 1003 ¶ 137). Referring to its showing with respect to the preamble, Petitioner contends that “data blocked by Duvall’s filtering system, as well as those not matching any filters, are ‘potentially security-related events represented in the status data’ because they may relate to requests for, or transmissions of, ‘indecent material,’ which may be

IPR2023-00889

Patent 7,895,641 B2

illegal (e.g., ‘outlaw[ed]’) and/or threaten the security of the requesting user or client device.” *Id.* at 35–36 (quoting Ex. 1004, 1:7–24; citing Ex. 1004, 4:61–64 (“[A]dvis[ing] the user on how to get back to the state before the user tried to open the stream and send the message.”)). Petitioner further argues that the ’641 patent does not limit the scope of what “security-related” encompasses, because the ’641 patent states that “the present invention is usable generally for [] monitoring of any system.” Reply 4 (citing Ex. 1001, 15:63–16:5; Pet. 8).

Petitioner alternatively relies on Chu as teaching determining “potentially security-related events” and suggesting the same in Duvall’s system. Pet. 36–37. That is, Petitioner argues that “Chu’s blacklists, which contain lists of ‘Web sites that serve potentially dangerous active codes,’” suggest the modification. *Id.* at 36 (quoting Ex 1005, 44; citing Ex. 1005, 23 ((discussing virus-ridden downloadable content))). Petitioner relies on Dr. Jeffay, summarizing his testimony as “explain[ing] that Duvall’s and Chu’s filtering techniques apply equally well in other security contexts, such as malware or intrusion detection, without needing any modifications.” *Id.* citing Ex. 1003 ¶ 138). In other words, “[f]ilters would include, for example, IP addresses or other criteria (e.g., URLs) associated with malware or potentially security-related content.” *Id.* (citing Ex. 1003 ¶ 138). Petitioner contends that “[a]pplying Duvall’s techniques in this manner amounts to nothing more than use of known techniques to improve similar devices, methods, or products in the same way (e.g., to detect malware or a potential intrusion instead of objectionable material).” *Id.* (citing Ex. 1003 ¶ 138; *KSR*, 550 U.S. at 417). Petitioner also contends that Chu’s black and white lists are similar in operation and function to Duvall’s BLOCK and ALLOW filters. *Id.* at 20. Petitioner contends that a person of ordinary skill

IPR2023-00889

Patent 7,895,641 B2

in the art would have turned to Chu in order to “more accurately resolv[e] residue data to ensure transmissions are correctly blocked or allowed.” *Id.* (citing Ex. 1003 ¶ 107). Petitioner also contends that in light of Chu’s teachings for a separate analysis for data neither allowed nor blocked, a person of ordinary skill in the art “would have recognized that information about data transmissions not matching any of Duvall’s filters could be provided to a user with only minor changes to Duvall’s overall process.” *See id.* at 23 (citing Ex. 1003 ¶ 114).

Patent Owner disputes Petitioner’s interpretation of claim 1 and disputes that Duvall and Chu analyze post-filtered status data to identify a potentially security-related event. Prelim. Resp. 34–42. According to Patent Owner, “both Duvall and Chu only teach filtering for things that are already known,” but “[n]either of them analyzes any data to identify *potential* threats after filtering (*i.e.*, previously unknown threats from the post-filtering residue).” *Id.* at 34. Patent Owner argues that “Petitioner improperly equates Duvall’s subjective-criteria based filtering . . . to an analysis that identifies events that are potentially objectively malicious.” *Id.* at 39. Patent Owner also argues that “[t]he status of Duvall’s data (including data ‘neither ALLOWED nor BLOCKED’) is always known to the user because the user subjectively pre-determines whether it is objectionable.” *Id.* (citing Ex. 2001 ¶ 147–148). Patent Owner also argues that even if “certain filtered content ‘can carry viruses or malware,’ . . . filtering the content would not amount to identifying the security-related events.” *Id.* at 40 (quoting Pet. 24). Patent Owner also argues that “Petitioner completely ignores that this first level analysis must be of status data—not just any data involved in the filtering process.” *Id.* at 39.

IPR2023-00889

Patent 7,895,641 B2

At this stage of the proceeding, Petitioner sufficiently shows that Duvall in combination with the teachings of Chu would have rendered this limitation obvious to a person of ordinary skill in the art. The term “potentially security-related events” is broad enough to encompass the objectionable material that Duvall monitors and/or those that Chu monitors, even if known or subjective. Dr. Jeffay credibly explains that Duvall’s and Chu’s similar technique for identifying objectionable material identifies potential and virus- and malware-related risks. *See* Ex. 1003 ¶¶ 113–115, 137–138. As Petitioner shows, Duvall’s filtering as supplemented by Chu’s teachings analyzes status data (including IP addresses) to identify potentially-related security events by blocking specific IP addresses and/or by further analyzing post-filtering residue data with further keyword and pattern matching search techniques and further using an analyst system as described below in connection with limitation 1.c *See* Pet. 39–30, 34, 37–40. We address similar arguments by Patent Owner below. *See infra* § III.A.1.vii (discussing rationale to combine).

Based on the preliminary record and foregoing discussion, we determine that Petitioner sufficiently shows for purposes of institution that the combination of Duvall and Chu teaches limitation 1.b.

iv) 1c) “a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system”

Petitioner contends that Duvall and Chu collectively teach limitation 1.c, because, *inter alia*, a person of ordinary skill in the art would have looked to Chu to optimize the handling of unresolved residue data in order to avoid “filtering too much or too little” in Duvall.” Pet 37 (citing Ex. 1004, 8:6–8; Ex. 1003 ¶¶ 140–141). Petition argues that “[i]n the case of

IPR2023-00889

Patent 7,895,641 B2

unresolved data, Chu prompts for human intervention,” which “would take the form of an analyst system having people trained to manage Duvall’s corporate network.” *Id.* at 37–38 (citing Ex. 1004, 8:18–23; Ex. 1005, 44 (“Prompt me for my attention”); Ex. 1003 ¶ 137).

Petition further argues that Duvall’s use of “*uniform set of filters form many users*” for “a corporate network” means that “the decision of how to handle unresolved data would not be left to each user individually, but rather, to a group of people trained in making such decisions, such as analysts at a network-security service.” *Id.* at 39 (quoting Ex. 1004, 8:18–23; citing Ex. 1003 ¶¶ 138–139). Petitioner also asserts that Duvall discloses a “password protected” “editing manager,” which suggests that persons editing filters in a corporate network are trained professionals. *Id.* at 38 (citing Ex. 1004, 8:8–10; Ex. 1003 ¶ 139). Therefore, Petitioner concludes that “in the Duvall-Chu combination, information about the unresolved residue data would be sent to a trained network analyst for handling of the unresolved residue data.” *Id.* at 39–40.

Petitioner further explains that “[t]his group of trained professionals responsible for maintaining uniformity of the filters is ‘an analyst system . . . associated with said security monitoring system,’” and a person of ordinary skill “would have been motivated to assign the role of managing and editing filters to a group of people having the expertise to properly evaluate whether ‘the filtering system is filtering too much or too little,’ rather than the individual receiving the illicit content.” Pet. 39–40 (quoting Ex. 1004, 8:6–8; Ex. 1003 ¶ 144).

Patent Owner argues that “[n]either Duvall nor Chu performs a first analysis, after filtering, on postfiltering residue, to flag potential events, at the probe, before transmission on for more detailed analysis.” Prelim. Resp.

IPR2023-00889

Patent 7,895,641 B2

37 (citing Ex. 2001 ¶¶ 141–155). Patent Owner contends that this first level analysis is in limitation 1.b, as follows: “analyze status data to identify potentially security-related events represented in the status data.” *Id.*

According to Patent Owner, a second level analysis is in “relevant language” of limitation 1.c, namely, “transmit information about the identified events to an analyst system associated with the security monitoring system.” *Id.* at 42 (citing Ex. 2001 ¶ 157). Patent Owner explains that “neither asserted reference provides even the slightest suggestion to transmit information about previously identified events from a first-level of analysis to an analyst system *that can determine whether the potential events are actual events and/or resolve them.*” *Id.* at 42–43 (citing Ex. 2001 ¶ 157) (emphasis added). Patent Owner further argues that “[t]o the extent there is any sort of analysis taught by the references (which there is not), analysis could only relate to the first level analysis—and not the second.” *Id.* at 43. Patent Owner also argues that “Duvall is silent as to any second-level of analysis.” *Id.*

According to Patent Owner, Chu does not fill the gaps in Duvall regarding transmitting to an analyst because (1) Chu does not have a first level of analysis that would trigger transmission to an analyst and (2) Chu does not “transmit” information to an analyst, Chu “simply returns control back to the end-user.” *Id.* at 43–44.

Patent Owner also contends that “Petitioner’s attempt to argue that ‘user intervention’ is the same as ‘transmitting information about said identified events to an analyst’ fails.” Prelim. Resp. 44 (citing Pet. 21–23; 37–40). According to Patent Owner, “[d]eferred control back to the application due to an inability to make a trust decision is different than transmitting information about identified potentially security-related events

IPR2023-00889

Patent 7,895,641 B2

to an analyst system (e.g., for a confirmatory analysis).” *Id.* (citing Ex. 1001, 2:36–43). Patent Owner also argues “[n]or would it make sense to redirect the alert away from the end-user to a (non-existent) analyst for any reason.” *Id.* (citing Ex. 2001 ¶ 157).

Patent Owner’s arguments regarding the “second-level of analysis” are not commensurate in scope with claim 1. *See* Prelim. Resp. 42–44. Step 1.c does not require the “analyst system” to analyze information, let alone perform a “second-level of analysis.” Rather, it merely requires “a communications system coupled to transmit information about the identified events to an analyst system.” The thrust of Patent Owner’s arguments rest on the faulty premise that the analyst system recited in limitation 1.c provides a “second-level of analysis.” *See id.* at 42–47.

Patent Owner’s arguments also attack Chu individually, which does not undermine the Petition, because the Petition relies on the combined teachings of Chu and Duvall to teach or suggest an analyst system. Patent Owner acknowledges that Chu “alerts the end-user of the lack of any determination.” Prelim. Resp. 45–46. Contrary to Patent Owner’s related arguments about Chu (*see id.*) and Duvall, this alert provides information to a user about an identified event from Chu’s, thereby suggesting feedback with respect to Duvall’s filtering analysts using an editing function on a corporate network, i.e., providing information relative to the first-level analysis to corporate analysts who may provide a second-level analysis (in Patent Owner’s parlance). *See* Ex. 1004, 8:1–25, Ex. 1005, 44. Duvall’s system explicitly provides feedback regarding blocked messages to a user’s screen. Ex. 1004, 6:62–65.

Patent Owner otherwise agrees that “[a]t best, Chu’s ‘user intervention’ teaches prompting the end-user for attention at the original

IPR2023-00889

Patent 7,895,641 B2

application.” Prelim. Resp. 46. In other words, this alert informs the end user/analyst system as suggested by the combination of Duvall and Chu that the previous filtering operations (ALLOW/BLOCK in Duvall or white list/black list in Chu) are unable to render a decision regarding a specific website, thereby suggesting further analysis as occurs in Duvall’s system and raising the issue of whether that website is potentially unsafe, as Petitioner argues. *See* Pet. 37–40.

Patent Owner also argues that the Petition fails to provide a reason as to

why it would have been obvious to (1) shift the prompts away from the end-user to the administrator, (2) modify those alerts to include information about identified potential security-related events rather than returning “*unknown*”, or (3) have the administrator that handles filters do double-duty to analyze security-related events.

Prelim. Resp. 46. This argument does not address the reasons advanced in the Petition as to “why.” For example, Petitioner argues it would have been obvious to implement Chu’s similar system and notify a security analyst “to optimize the handling of unresolved residue data in order to avoid ‘filtering too much or too little’ in Duvall.” Pet 37 (citing Ex. 1004, 8:6–8; Ex. 1003 ¶¶ 140–141). And as noted above, Petitioner further explains that the combined teachings suggest employing trained network security analysts to handle a group of corporate filters, which further optimizes and uniformly handles unresolved data as opposed to leaving decisions about individual filters and associated websites to untrained single operators whose decisions may not be uniform (i.e., contradict each other). *See id.* at 37–40.

Contrary to Patent Owner’s argument that “Petitioner never explains how these modifications would be made,” Patent Owner recognizes that “the

IPR2023-00889

Patent 7,895,641 B2

administrator that handles filters [e.g., using Duvall’s editing manager] do[es] double-duty to analyze security-related events.” See Prelim. Resp. 46. And as noted above, limitation 1.c is broad, and does not require the “analyst system” to analyze information.

Based on the preliminary record and foregoing discussion, we determine that Petitioner sufficiently shows for purposes of institution that the combination of Duvall and Chu teaches limitation 1.c.

v) “*d) a receiver for receiving feedback at the probe based on empirically derived information reflecting operation of the security monitoring system*”

Referring to its showing for limitation 1.c, Petitioner contends that the combined teachings of Duvall and Chu teach this element, asserting that “information about residue data is sent to an analyst for handling.” Pet. 40. Petitioner also contends that Duvall “discloses feedback in the form of an ‘editing Manager’ that allows ‘edit[ing] the database to add, delete, or modify filters in the database.” Pet. 41 (alteration in original) (quoting Ex. 1004, 8:2–5). According to Petitioner, a person of ordinary skill in the art would have recognized that

Duvall’s editing manager provides “*a receiver for receiving feedback . . . based on empirically-derived information reflecting operation of said security monitoring system*” because the information is only provided to the trained professional if the data is residue data—meaning that the data did not match any allow/block filters and passed through subsequent analysis (e.g., keywords and pattern matching) without any resolution.

Id. (citing Ex. 1004, 5:8–18; Ex. 1003 ¶¶ 146–147). As indicated above in connection with limitation 1.c, Petitioner relies on Chu’s teaching of providing “[u]ser intervention [to a user/analyst]. . . only when the given URL is neither the blacklist nor the whitelist” to suggest providing feedback

IPR2023-00889

Patent 7,895,641 B2

information arising from the analyst's receipt of information about the filtering process and including residue data, where Chu also teaches prompting the user/analyst when there is neither blocking nor allowing of status data. *See id.* at 39 (quoting Ex. 1004, 44 (“Prompt me for my attention otherwise.”)).

That is, Petitioner argues that “decisions made by the trained professional (e.g., whether the filters should be modified) would be based on observable information about the data (e.g., transmission path, URL, etc.).” Pet. 40 (citing Ex. 1003 ¶ 147). Petitioner adds that “[f]eedback is received ‘at the probe’ because Duvall’s editing manager is part of the filtering system implemented on server 30.” *Id.* (citing Ex. 1004, 8:2–5, 8:18–21; Ex. 1003 ¶ 148).

Patent Owner argues that “Duvall’s filters are modified based on the user’s ‘belie[f] that the filtering system is filtering too much or too little[,]’ [b]ut subjective beliefs and the user’s ‘individual tastes and sensitivities’ are not objectively verifiable.” Prelim. Resp. 49 (quoting Ex. 1004, 8:7, 2:15–16). According to Patent Owner, this shows that “Duvall’s feedback is therefore based on the exact opposite of ‘empirically-derived information.’” *Id.* (citing Ex. 2001 ¶ 178). Even if the claims somehow preclude “subjective beliefs” and Duvall relies partly on same, this line of argument does not undermine Petitioner’s showing that the analyst system of the combined teachings as proposed by Petitioner relies on feedback information about residue data as data that the system did not allow or block, as

IPR2023-00889

Patent 7,895,641 B2

Petitioner shows (Pet. 41), and as also discussed in the previous section in connection with the analysis of transmitted information of limitation 1.c.⁹

Patent Owner advances related arguments that relate to Petitioner’s showing with respect to limitation 1.e, discussed in the next section. *See* Prelim. Resp. 47–48 (grouping limitations 1.d and 1.e together).

Based on the preliminary record and foregoing discussion, we determine that Petitioner sufficiently shows for purposes of institution that the combination of Duvall and Chu teaches limitation 1.d.

vi) “(e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback”

Referring to its showing for limitations 1.c and 1.d, Petitioner contends that the combination of Duvall and Chu teach limitation 1.e because, *inter alia*, the combination teaches “‘receiving feedback’ from an analyst via Duvall’s ‘editing Manager,’ which ‘allows the user to edit the database to add, delete, or modify filters in the database.’” Pet. 41 (non-emphasized quotes quoting Ex. 1004, 8:2–5; citing Pet. § VI.A.2(3); Ex. 1003 ¶ 149).

According to Petitioner, “[e]diting the filters in Duvall’s filter database ‘*modif[ies] an analysis capability of said probe . . . based on said feedback*’ because Duvall operates by comparing ‘information in the data

⁹ It is not clear on this preliminary record if “empirically derived information” as recited in limitation 1.d refers back to, or further limits, the recited “information” in limitation 1.c. On this preliminary record, limitation 1.d may further limit limitation 1.c, but it need not do so (claim 1 is agnostic). For example, both limitations recite “information” but limitation 1.d does not specify that limitation 1.c’s “information” provides an antecedent for limitation’s 1.d’s “empirically-derived information” (e.g., using “the” or “said” in relation to “information”).

IPR2023-00889

Patent 7,895,641 B2

stream to the filter entries stored in the database to determine whether some action needs to be taken.” Pet. 41 (second quote quoting Ex. 1004, 4:22–27; citing Ex. 1004, 4:27–30, 4:40–43). According further to Petitioner, “Duvall’s system searches filters in the database when determining whether to allow or block a data transmission.” *Id.* (citing Ex. 1003 ¶ 150). “As filters are added, deleted, or modified, Duvall’s analysis would reflect these updates.” *Id.* (citing Ex. 1004, 8:3–16; Ex. 1003 ¶ 150).

Petitioner also contends that “Duvall’s filtering system accommodates dynamic updates because it searches ‘filter entries stored in the database’ when performing its analysis, . . . which would reflect changes to filters as they are edited.” Pet. 42 (quoting Ex. 1004, 4:25–26; citing Ex. 1004, 4:22–43, 8:3–16; Ex. 1003 ¶ 152). Petitioner also asserts the following:

Duvall recognizes that “[b]ecause Internet sites are being added to the Internet at a fast rate . . . the filtering system preferably also has an updating mechanism to keep filters current” and that “the system can adapt as new sites and servers are added to the Internet.” EX1004, 7:18–21; 2:16–18. Given the rapidity of updates, a POSA would have recognized that Duvall’s “*analysis capability of said probe*” is “*dynamically modified . . . during operation thereof*” because taking the system offline each time an update was required would be disadvantageous. EX1003, ¶151. To avoid this disadvantage, Duvall “provid[es] updates online” so that “the system can adapt as new sites and servers are added to the Internet.” EX1004, 2:16–18.

Pet. 41–42.

Petitioner asserts that “[a] main benefit of databases is that entries can be edited or added without taking the system offline, which prevents the filtering system from being down during updates.” Pet. 42 (citing Ex. 1003 ¶ 153). Petitioner contends that “[s]ince Duvall’s system ‘searches the filter database for matching filters’ when opening a new data stream, the ‘analysis

IPR2023-00889

Patent 7,895,641 B2

capability of said probe’ always reflects the latest and current set of filters.”

Id. (quoting Ex. 1004, 4:40–43; citing Ex. 1003 ¶ 153).

Relying on a district court claim construction (Ex. 1013), Patent Owner argues that Duvall’s system is not “modified dynamically” because it does not “modify[] its analysis capability ‘during actual operation, rather than offline.’” Prelim. Resp. 48 (quoting Ex. 1013, 2). Addressing Petitioner’s argument that “the analysis capability of Duvall is modified dynamically ‘because taking the system offline each time an update was required would be disadvantageous,’” Patent Owner contends that “just because taking the system offline would be disadvantageous does not mean Duvall teaches modifying its analysis capability ‘during actual operation, rather than offline.’” *Id.* (citing Pet. 41; Ex. 1013, 2). According to Patent Owner, “the word ‘online’ in Duvall means ‘over the Internet’—not while the system is operational.” *Id.* at 49 (citing Ex. 2001 ¶ 174; Ex. 1004, 2:16–18; 7:17–29). Patent Owner also argues that “Duvall teaches pre-processing the database to ‘substantially reduce[]’ the number of comparisons made *when searching* the database during operation.” Prelim. Resp. 50 (quoting Ex. 1004, 9:11; citing Ex. 1004, 8:40–42, 9:9–11). Patent Owner argues that this searching process is incompatible with “dynamic” modification because it requires generating “two additional tables . . . whenever the filters are modified before searching is possible.” *Id.* (citing Ex. 1004, 8:39–62, 9:9–11; Ex. 2001 ¶¶ 176–177). Patent Owner also argues that “[t]he filtering system would be inoperable while the database performs the preprocessing.” *Id.* (citing Ex. 2001 ¶¶ 176–177).

Contrary to these arguments, Duvall’s system, like claim 1, does not require this relied-upon “preprocessing” for all embodiments of its server filter database. *See* Ex. 1004, 8:19–9:11 (describing an alternative

IPR2023-00889

Patent 7,895,641 B2

preferable embodiment). In addition, as discussed further below, claim 1 does not require modifying an analysis capability of the probe while the probe performs a search—the probe system may be operational prior to, or after, actually performing a search, for example, after it receives the feedback as limitation 1.e requires and then while simply waiting for input from one or more users designating a URL with its web browser. As Patent Owner shows, the '641 probe uses “sensors” and “monitors and collects information from any component providing status data” “derived from traffic.” *See* Prelim. Resp. 7–8 (citing Ex. 1001, 4:45–49, 5:50–54).

Similarly, Duvall’s system monitors a port for any data. *See* Fig. 3 (step 100 (“DATA STREAM OPENED?")). That is, as Petitioner contends, Duvall’s “filtering system *detects when the client opens the data stream for a particular port and IP address* (step 100), and searches the filter database for matching filters.” Pet. 30 (quoting Ex. 1004, 4:37–42 (emphasis added); citing Ex. 1003 ¶ 128). In other words, Duval’s filtering system is operational at step 100 of Figure 3, when it runs to detect “DATA STREAM OPENED?” prior to “search[ing] the filter database for matching filters” on a current search and also after a previous search. *See* Ex. 1004, 3:49–63, 4:37–42, Fig. 3 (step 100).

Moreover, claim 1 only requires that the modification control system *is capable of* “dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.”¹⁰ *See ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1361 (Fed. Cir. 2018) (“[A] prior art reference may anticipate or render obvious an apparatus

¹⁰ The parties do not contend that limitation 1.e (or other limitations) are means-plus-function terms under 35 U.S.C. 112, par. 6 at this stage of the proceeding.

IPR2023-00889

Patent 7,895,641 B2

claim—depending on the claim language—if the reference discloses an apparatus that is reasonably capable of operating so as to meet the claim limitations, even if it does not meet the claim limitations in all modes of operation.”). *ParkerVision* notes that previous Federal Circuit “cases distinguish between claims with language that *recites capability*, and those that *recite configuration*,” and “where claim language recites ‘capability, as opposed to actual operation,’ *an apparatus that is ‘reasonably capable’ of performing the claimed functions ‘without significant alterations’ can infringe those claims.*” *Id.* at 1362 (quoting *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1217 (Fed. Cir. 2014) (emphasis added)).

Here, claim 1 recites “a modification control system *for* dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback,” which, on this preliminary record, is the same as citing mere “capability.” *See id.* at 1362 (holding that claims reciting “[a]n apparatus *for frequency up-conversion*” (claim 4) or “[a]n apparatus *for communicating*” merely recite a capability). “As a result, ‘[a]n invention need not *operate* differently than the prior art to be patentable, but need only *be* different’—or, rather, ‘*unobviously* different.’” *Id.* at 1361 (quoting *Hewlett-Packard Co. v. Bausch & Lomb Inc.*, 909 F.2d 1464 & n.2, 1468 (Fed. Cir. 1990)); *see also In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997) (“It is well settled that the recitation of a new intended use for an old product does not make a claim to that old product patentable.”); *In re Anderson*, 662 F. App’x 958, 963 (Fed. Cir. 2016) (nonprecedential) (“We also agree with the Board that the ‘for use’ claim language is a statement of intended use. The ‘for use’ language does not add a structural limitation to the claimed system or method.”).

IPR2023-00889

Patent 7,895,641 B2

In other words, to meet limitation 1.e, Duvall’s client processor 20 and editing manager (under Petitioner’s showing) need only be “reasonably capable” of accessing filter database 24 at server 30 or (RAM at the client (which downloads the filter database)) to modify same, while the processor’s implementing software monitors a port as it does at step 100 of Figure 3. *See* Ex. 1004, code (57), 2:1–11, Figs. 1–3; *ParkerVision*, 903 F.3d at 1362 (quoting *Ericsson, Inc.*, 773 F.3d at 1217)). That is, in Duvall’s system, “[t]he client *monitors . . . ports* and maintains internal tables that indicate the state of each active TCP data stream, *whether that stream is open or closed*, for both incoming and out going transmissions.” *Id.* at 3:59–63 (emphasis added); *see also* Pet. 30 (quoting Ex. 1004, 4:37–420, Fig. 3 (step 100 (“DATA STREAM OPENED?”)). So when a data stream is closed and the system is monitoring the ports to see if “DATA STREAM OPENED?,” Duvall’s probe is operational.

As indicated above, Petitioner relies on the following editing manager functions as the “modification control system for dynamically modifying an analysis capability of the probe during operation thereof”:

The implementation and use of the editing manager are generally based on known database editing techniques. In addition, during a session over the Internet, a user can copy URLs for later editing. The user can then copy those URLs for inclusion in the database, or can edit the entry, e.g., to change the action from allow to block or vice versa

Ex. 1004, 8:11–16.

Petitioner also cites to Duvall’s updating mechanism “to keep the filters current” because “Internet sites are being added to the Internet at a fast rate.” Ex. 1004, 16–21; *see* Pet. 41 (citing same). This “updating mechanism causes the filtering system to download from the update server

IPR2023-00889

Patent 7,895,641 B2

one of a number of new sets of filters, and preferably causes some or all of the existing filters in the filter database to be replaced with the newly downloaded filters.” *Id.* at 7:24–28. Duvall does not explicitly limit its updating mechanism to require the probe filtering system’s processor and implementing software not to be operating (i.e., monitoring a data stream, step 100, Fig. 3), while it performs updates. *See id.* at 1:26–29, 3:43–46 (“Processing by the filtering system is carried out by the computer’s processor 20, and the system uses the computer’s storage 22 to store a filter database.”); 7:15–67 (describing updating mechanism of the “filtering system” from an update server (i.e., on the Internet)—instead of describing only updating of the filter database without monitoring a port).

Patent Owner contends that Duvall’s editing manager is only operational “for **later editing**” after a user copies a URL and argues that this does not support Petitioner’s alleged reliance on “inherency” in Duvall’s database system for allowing updates while the system is “operational.” *See* Prelim. Resp. 48–49. Patent Owner otherwise does not dispute that Duvall’s updating mechanism (described above) provides for filter updates while the system is on the Internet. *See id.* at 49 (“Merely updating over the Internet (i.e., online) neither teaches *nor suggests* ‘dynamically’ modifying an analysis capability ‘during actual operation, rather than offline.’” (emphasis added)). And Duvall describes that “[t]he editing filter allows the user to make custom changes if the user believes that the filtering system *is* filtering too much or too little.” Ex. 1004, 8:5–8 (emphasis added). Duvall does not explicitly describe that a user/analyst cannot make BLOCK or ALLOW changes to a stored URL while the system is monitoring client ports for data transmissions input by the user/analyst, even if Duvall

IPR2023-00889

Patent 7,895,641 B2

describes the “addition[al]” capability of allowing a user to “copy URLs” to make “later editing” changes to the filtering system. *See id.* at 8:1–16.

On this preliminary record, Petitioner sufficiently shows that Duvall’s editing manager is reasonably capable of allowing dynamic modifications of an analysis capability as limitation 1.e requires, even if Duvall does not explicitly disclose such a capability. Duvall generally discloses “a filtering database and *implementing software* can be stored on a server in a network to which a client is coupled.” Ex. 1004, 1:61–62 (emphasis added). In other words, Duvall’s “implementing software” controls access to the filtering database.¹¹ As an option, Duvall discloses that the “filter database” “could be copied to RAM during operation.” *See id.* at 3:48–49. This implies that Duvall’s editing manager is reasonably capable of accessing RAM or the filtering data base to perform editing upgrades. The fact that Duvall describes that “[i]n *addition*, during a session over the Internet, a user can copy URLs for later editing” does not show that later editing means a user must shut down Duvall’s “implementing software” to perform filter edits. *See* Ex. 1004, 1:61–62, 2:3–5, 8:11–16 (emphasis added).

Other general descriptions in Duvall support this preliminary finding. For example, Duvall discloses that “[t]he system periodically accesses the update server over the Internet, and downloads one of a number of new sets of filters from the server *to replace some or all of the existing filters.*” *Id.* at 1:55–58 (emphasis added). Prior to this description, Duvall generally discloses that the “*system . . . allows Internet users to filter material transmitted over the Internet.*” *Id.* at 1:28–29 (emphasis added). On this

¹¹ On this preliminary record, it appears that the implementing software also may reside on one or more of the client computers, with the filter database stored on the server. *Compare* Ex. 1004, 1:60–62, *with* 8:18–26.

IPR2023-00889

Patent 7,895,641 B2

preliminary record, this sufficiently shows a form of dynamic modification of the filters during filtering by the “*system*,” while the “*system*” is operational and on the Internet (“on-line”). On this preliminary record, the system is reasonably capable of operating the probe while periodically downloading uploads, because such downloads at least access the filter database, which the implementing software controls. *See id.* at 1:28–29, 55–58, 61–62.

Duvall also discloses a web browser to access web sites (*id.* at 2:63–65), and that that processor is capable of “multi-tasking” (*id.* at 1:67). Duvall also discloses that “the present invention uses patches to inject filtering code into RAM without modifying or replacing the library on the disk.” *Id.* at 2:3–5. “Because the library is not replaced or modified, *the system can adapt to upgrades or reloading* without the concern of losing modified or alternate variations of programs.” *Id.* at 2:8–11 (emphasis added).

As noted above, Patent Owner also argues that “Duvall teaches pre-processing the database to ‘substantially reduce[]’ the number of comparisons made when searching the database during operation,” which “is incompatible with ‘dynamic’ modification because . . . two tables need to be generated whenever the filters are modified before searching is possible.” Prelim. Resp. 50 (quoting Ex. 1004, 8:39–61; 9:9–11; Ex. 2001 ¶¶ 176–177). This argument fails to explain how pre-processing to create a search technique, according to one embodiment, undermines dynamic modification that may occur while the system operates (e.g., polls ports and provides filter updates when a user is not actively searching). Also, Duvall teaches that this relied-upon embodiment is for “an alternative search technique,” because other described techniques “may not be efficient enough.” Ex. 1004, 8:38–

IPR2023-00889

Patent 7,895,641 B2

42. As Patent Owner recognizes, Duvall’s alternative searching technique ultimately “minimize[s]” “the number of full string comparisons which need to be made.” *Id.* at 8:66–67. Nevertheless, even if a user is searching while the system is operational (which claim 1 does not require on this preliminary record), the system does not necessarily employ this search technique to make simple modifications, because Duvall otherwise discloses “us[ing] the same the same type of filter database as a client-based filtering system, but the filter database is located on server 30.” *Id.* at 8:23–26.

Based on the preliminary record and foregoing discussion, we determine that Petitioner sufficiently shows for purposes of institution that the combination of Duvall and Chu teaches limitation 1.e.

vii) Rationale to Combine the Teachings of Duvall and Chu

Patent Owner raises a number of arguments asserting a failure of the Petition to show sufficient reasons to combine the teachings of Duvall and Chu with a reasonable expectation of success to arrive at the claimed invention. *See* Prelim. Resp. 51–67. We address various forms of most of these arguments above and address them further below.

For example, Patent Owner argues that Duvall’s system does not relate to security and only relates to censorship. Prelim. Resp. 53–54 (citing Ex. 1003 ¶ 103; Ex. 2001 ¶¶ 183–184). Patent Owner asserts that security concerns require “objective criteria.” *Id.* at 53. Patent Owner also argues that “Duvall’s filtering system is unsuitable as a security monitoring device,” and applying Chu “fundamentally transform[s] the nature of Duvall” and is “circular” reasoning. *Id.* at 55–56. Patent Owner also argues that “Duvall is unconcerned with the analysis of raw packet data.” *Id.* at 56.

Most of these arguments and similar arguments are beyond the scope of the challenged claims, because on this record, “security” does not require

IPR2023-00889

Patent 7,895,641 B2

“objective criteria” or analysis of raw packet data. Even if security requires objective criteria, as Petitioner shows, Chu’s and Duval’s filter systems each objectively determine if characters in the URL match those in the filter string. *See* Pet. 34–35, 37–38 (showing that both systems look for pattern or keyword matches (citing Ex. 1004, Fig. 4; Ex. 1005, 44)). The ’641 appears to operate similarly. *See supra* § II.C. The arguments also fail to undermine Petitioner’s reasons for combining the security systems of Chu and Duvall, some of which we address above in connection with limitation 1.b. *See* Pet. 13–26, 23–25, 38–40; *supra* § III.A.1.iii. Patent Owner also does not dispute Petitioner’s explanation that a person of ordinary skill “would have recognized that data transmissions from unknown or questionable sources [which Duvall’s system monitors] can carry viruses or malware, as noted, for example, by Chu.” *Id.* at 24. As Petitioner also explains, “illegal material,” which Duvall’s system blocks, is likely is a security concern for a networks. *See id.* And as explained above, the challenged claims require identifying “*potentially* security-related events.”

Patent Owner also argues that Petitioner’s motivation mischaracterizes Duvall’s teachings because “Duvall never suggests—as Petitioner implies—that its filtering systems would be inaccurate because the user was uncertain whether he believed something was objectionable.” Prelim. Resp. 58 (citing Pet. 19). Patent Owner also argues that Duvall does not “contemplate any techniques or analysis that could assist with that determination.” *Id.* Petitioner also argues that “Duvall presents” an editing manager “as the solution to the problem of ‘filtering too much or too little,’” so that a person of ordinary skill “would not actually seek any objective analysis techniques as Petitioner suggests.” *Id.* at 59 (citing Pet. 23–24, 38–41). On this preliminary record, these arguments do not undermine

IPR2023-00889

Patent 7,895,641 B2

Petitioner's showing. The arguments generally assume that all users of Duvall's computers, and analysts with access to the editing manager, already know the status of all websites of concern and that new websites of concern do not arise. As summarized above, Petitioner sufficiently shows that the Duvall-Chu' users and analysts would have benefited from input by experienced security analysts in order to help determine if websites are of potential concern and to modify filters accordingly.

Patent Owner also argues that "the resulting combination Petitioner proposes would still flood the analyst system with an unmanageable amount of information" and render the combination "inoperable." Prelim. Resp. 67. This argument is beyond the scope of the challenged claims, because the claims do not require a minimal amount of information to analyze. In addition, the claimed combination does not specify how often the computers in a network search, or how many computers are in the "computer network," wherein users ultimately control the number of searches that the system monitors.

Patent Owner also argues that "Chu does not tune filters with 'user intervention.'" Prelim. Resp. 64. It is not clear how this argument relates to a claim limitation or how it relates to Petitioner's showing, which relies on the combined teachings of Chu and Duvall. Patent Owner's related arguments regarding "what Chu means by 'user intervention'" attack Chu individually, and do not undermine the Petition, which relies on the combination of Chu and Duval. *See id. at 63–64; see also id. at 62* (arguing "Chu does not teach . . . features" that the Petition argues that the combination of Chu and Duvall teaches).

Patent Owner similarly argues that "Chu is silent about any techniques to analyze residue from . . . filters." *Id. at 61*. Nevertheless, as discussed

IPR2023-00889

Patent 7,895,641 B2

above, Petitioner generally relies on Chu as suggesting that Duvall's residue data may benefit from more analysis to resolve, because Chu's similar filtering system prompts the user, suggesting that experienced users employ further intervention to resolve security questions. *See* Pet. 37–40.

Patent Owner also argues that Chu and Duvall “use their filters for different purposes,” including that “Chu uses filters to determine trust, Duvall only teaches a filtering system for censoring—but makes no objective determinations.” Prelim. Resp. 59. Patent Owner also argues that “Duvall and Chu's perspectives on ‘trust’ are diametrically opposed,” because Duvall's system trusts the system and Chu's system trusts the user. *Id.* at 60–61. Contrary to these arguments, however, as Petitioner notes, Duvall's system includes an editing manager with optional password protection, suggesting mechanisms for verifying trust of some of its users/analysts. *See* Pet. 38 (citing Ex. 1004, 8:8–10; Ex. 1003 ¶ 142). Moreover, as explained above, characterizing Duvall's comparison of URL sites to filters as subjective is not a fair characterization, because the filter system objectively determines if characters in the URL match those in the filter string, similar to the system of Chu. *See* Pet. 34–35, 37–38 (showing that both systems look for pattern or keyword matches (citing Ex. 1004, Fig. 4; Ex. 1005, 44)).

Based on the preliminary record and foregoing discussion, we determine that for purposes of institution, Petitioner sufficiently provides reasons for the combination with a reasonable expectation of success.

vii) Summary of Claim 1

Based on the preliminary record and foregoing discussion, we determine that Petitioner demonstrates a reasonable likelihood of showing that claim 1 would have been obvious.

IPR2023-00889

Patent 7,895,641 B2

2. *Analysis of Claims 2–7 and 15–17*

Having reviewed Petitioner’s arguments and supporting evidence in this preliminary record, including the arguments summarized above for claim 1, we determine Petitioner sufficiently shows for purposes of this Decision that the combination of Duvall and Chu would have rendered claims 1–7 and 15–17 obvious. *See* Pet. 42–49. Patent Owner does not address Petitioner’s showing with respect to these claims. *See generally* Prelim. Resp. Based on the preliminary record, we determine Petitioner demonstrates a reasonable likelihood of showing that these claims would have been obvious.

B. Alleged Obviousness of Claims 7–13 and 16 in view of Duvall, Chu, and Trcka

Having reviewed Petitioner’s arguments and supporting evidence in this preliminary record, including the arguments summarized above for claim 1, we determine Petitioner sufficiently shows for purposes of this Decision that the combination of Duvall, Chu, and Trcka would have rendered these claims obvious. *See* Pet. 50–57. Patent Owner does not address Petitioner’s showing with respect to these claims. *See generally* Prelim. Resp. Based on the preliminary record, we determine Petitioner demonstrates a reasonable likelihood of showing that these claims would have been obvious.

C. Alleged Obviousness of Claims 14 and 15 in view of Duvall, Chu, Trcka, and Ziese

Having reviewed Petitioner’s arguments and supporting evidence in this preliminary record, including the arguments summarized above for claim 1, we determine Petitioner sufficiently shows for purposes of this Decision that the combination of Duvall, Chu, Trcka, and Ziese would have

IPR2023-00889

Patent 7,895,641 B2

rendered these claims obvious. *See* Pet. 58–63. Patent Owner does not address Petitioner’s showing with respect to these claims. *See generally* Prelim. Resp. Based on the preliminary record, we determine Petitioner demonstrates a reasonable likelihood of showing that these claims would have been obvious.

D. Alleged Obviousness of Claims 18–25 in view of Duvall, Chu, and Cogger

Petitioner contends that claims 18–25 would have been obvious to person of ordinary skill in the art in view of the combined teachings of Duvall, Chu, and Cogger. Pet. 67–84. Claim 18 is independent. *See supra* § II.D (reproducing claim 18). Claims 19–25 depend from claim 18. Patent Owner disputes Petitioner’s contentions with respect to independent claim 18. Prelim. Resp. 67–69.

The preamble and first step of claim 18 follow:

18, A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:

creating an event record for information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering;

Petitioner primarily relies on its analysis of claim 1 as outlined above to address the above preamble and the first step of claim 18. *See* Pet. 67–69 (citing Pet. § VI.A..2(a)). With respect to the “secure operations center” as recited in the preamble, to the extent it is limiting, Petitioner reads it partly on Cogger’s Customer Service Management System (CSM), which receives trouble tickets from different security analysts at corporate networks in the Duvall-Chu system, in order to better track, evaluate, and resolve security

IPR2023-00889

Patent 7,895,641 B2

issues, as described further below. *See id.* at 65–67 (citing Ex. 1033, 2:50–3:3, 3:65–66; Ex. 1003 ¶¶ 224–230). With respect to the recited “event record” recited in the first step of claim 18, Petitioner also asserts that a person of ordinary skill “would have understood that the transmitted information [in the Duvall-Chu system and as recited in limitation 1.c] is ‘an event record’ because it is information about the network event.” *Id.* at 69 (citing Ex. 1003 ¶ 232). Patent Owner does not particularly dispute this showing, other than as discussed below. *See* Prelim. Resp. 67–69.

Claim 18 also recites the following “event record” and “trouble ticket” limitations, which involve correlating and organizing information into a “problem ticket” and sending same to a “security analysis console”:

correlating the event record with customer information and a symptom record;

using the correlated symptom record to link the event record to problem resolution information;

consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket; and

providing the problem ticket to a security analyst console for analysis.

To address the above limitations, Petitioner turns to Cogger for its “trouble ticket techniques” and incorporates them into “Duvall-Chu’s system to prompt a network administrator, as disclosed in Cogger, to resolve residue data transmissions.” *See* Pet. 67 (citing Ex. 1003 ¶ 228; *supra* § II.I.5 (summarizing Cogger’s teachings)).

Petitioner contends that “Cogger discloses ‘*operating a secure operations center*’ in the form of a ‘Customer Service Management System’ (CSM) that receives trouble tickets transmitted from customers.” Pet. 67 (second quote quoting Ex. 1033, 3:65–66; citing Ex. 1003 ¶ 229). Petitioner

IPR2023-00889

Patent 7,895,641 B2

relies on Cogger’s “disclos[ure] that communication between customers and the CSM is ‘secure,’ providing ‘secure web servers and back end services to provide applications that establish user sessions . . . and communicate with adaptor programs to simplify the interchange of data across the network.’” *Id.* (citing Ex. 1033, 5:46–50, 7:55–60 (describing secure TCP messaging over secure Internet paths)).

Petitioner explains that “[i]n the Duvall-Chu-Cogger system, Cogger’s CSM would be implemented as part of Duvall-Chu’s network-administrator resolution pathway for receiving and analyzing tickets transmitted from subscriber networks.” Pet. 68 (citing Ex. 1003 ¶ 230; Pet. § VI.D.1). According further to Petitioner, “Duvall-Chu-Cogger’s residue data-review system, like Cogger’s CSM, provides “a secure operations center as part of a security monitoring system for a customer computer network.” *Id.* (citing Ex 1003 ¶ 230). Petitioner adds that a person of ordinary skill in the art “would have been motivated to ensure personnel operating Duvall-Chu-Cogger’s service were doing so securely because the service would receive network activity from private customer networks (e.g., ‘a corporate network’).” *Id.* (citing Ex. 1004, 8:21–23; Ex. 1003 ¶ 231).

Petitioner adds that a person of ordinary skill in the art “would have been motivated to incorporate such information into a ‘trouble ticket,’ as in Cogger, to efficiently and coherently provide the information to a trained professional (e.g., Cogger’s network administrators).” Pet. 69 (citing Ex. 1003 ¶ 233.” Petitioner also argues that “[t]he information as recorded in the trouble ticket thus also provides ‘an event record.’” *Id.* (citing Ex. 1003 ¶ 233).

Petitioner generally reads the remaining steps, i.e., the “correlating” step, the “using” step,” the “consolidating” step, and the “providing” step,

IPR2023-00889

Patent 7,895,641 B2

onto Cogger's ticket teachings. *See* Pet. 69–75. Patent Owner does not dispute Petitioner's reading of Cogger, which is sufficient on this record for purposes of institution. *See* Prelim. Resp. 67–69.

Rather, Patent Owner argues that “[t]here is no motivation to combine Cogger into Duvall-Chu.” Prelim. Resp. 67. Patent Owner characterizes Cogger's system as “allow[ing] customers to remotely access a pre-existing system through its disclosed interface,” which is “not the same as using the underlying system to remotely manage a filtering database.” *Id.* at 68 (citing Ex. 2001 ¶ 226). Patent Owner argues that Petitioner “modifies Duvall-Chu to do just that.” *Id.* Patent Owner explains that “Petitioner's combination first requires Duvall-Chu to utilize remote management before a trouble ticketing system for that remote management even begins to make sense.” *Id.* According to Patent Owner, “that teaching is absent from Duvall, Chu, and Cogger.” *Id.*

Patent Owner also argues that Petitioner does not explain why a person of ordinary skill “would look at Cogger in the first place.” Prelim. Resp. 68. Patent Owner also argues that “Petitioner also provides no details about how Cogger could even be combined into Duvall-Chu with a reasonable expectation of success.” *Id.* at 69. Patent Owner also argues that Cogger does not disclose the specifics of the ticketing system so that a [person of ordinary skill] could implement one for Duvall-Chu.” *Id.* at 68. According to Patent Owner, “Cogger only teaches the interface to access that telecommunications ticketing system's pre-existing features.” *Id.*

Contrary to Patent Owner's assertion of “no motivation” and a lack of a reasonable expectation of success, Petitioner provides sufficient reasons on this preliminary record to turn to Cogger and implement Cogger's ticket teachings with Duvall-Chu's system with a reasonable expectation of

IPR2023-00889

Patent 7,895,641 B2

success. Pet. 64–67. For example, Petitioner argues that “Cogger’s trouble tickets would . . . provide a tracking mechanism to Duvall’s network administrators of each corporate network to assure residue data is resolved in a timely manner.” *Id.* at 66 (citing Ex. 1033, 2:50–3:3; Ex. 1003 ¶ 224). Petitioner also argues that a person of ordinary skill in the art “would have been motivated to incorporate Cogger’s techniques for generating and transmitting trouble tickets in Duvall-Chu’s system for use in prompting Cogger’s network administrators to resolve residue data.” *Id.* at 65 (citing Ex. 1003 ¶ 224). Petitioner also argues that “[t]ransmitting ‘trouble tickets’ with sufficient information about residue data to . . . network administrators would ensure that the service can appropriately evaluate and resolve such data transmission.” *Id.* at 65–66 (citing Ex. 1003 ¶ 224). Petitioner adds that “[t]his would allow . . . network administrators to efficiently update the corporation’s filter database as appropriate, adding new filters to address newly-discovered Internet sites.” *Id.* at 66 (citing Ex. 1003 ¶ 224).

Patent Owner also asserts that a person of ordinary skill in the art could not substitute Cogger’s “entire suite of applications . . . into Duvall-Chu with any reasonable expectation of success.” Prelim. Resp. 69. This argument incorrectly assumes that Petitioner must show a whole-sale bodily incorporation of Cogger’s entire system into the Duvall-Chu system to establish obviousness for institution purposes. Contrary to this line of argument, Petitioner sufficiently shows that a person of ordinary skill in the art “would have had a reasonable expectation of success incorporating Cogger’s techniques into Duvall-Chu’s system because this would amount to nothing more than incorporating well-known techniques (generating and transmitting tickets about network events) into Duvall-Chu’s known filtering system.” Pet. 66–67 (citing *KSR*, 550 U.S. at 419–421; Ex. 1003 ¶ 226).

IPR2023-00889

Patent 7,895,641 B2

In summary, Patent Owner's arguments do not address Petitioner's stated reasons and showing of a reasonable expectation of success with particularity and fail to undermine the Petition. *See* Prelim. Resp. 67–69.

Contrary to Patent Owner's argument that Cogger only teaches an interface and lacks specifics, Patent Owner contradicts itself by arguing that “Cogger relies on a complex pre-existing architecture and a suite of other pre-existing telecommunications applications.” Prelim. Resp. 69 (citing Ex. 1033, 1:32–36; 6:8–14; 13:66–14:17). Even if Cogger lacks certain specifics, the asserted lack of specifics is further evidence on this preliminary record that an artisan of ordinary skill already would have known how to implement Cogger's interface and ticketing system in Duvall-Chu's system with a reasonable expectation of success.

Regarding Patent Owner's arguments that Petitioner fails to show how to implement Cogger's teaching, based on an alleged “remote management” requirement in Duvall-Chu to implement Cogger's ticket system, claim 18 does not recite such a requirement. Rather, claim 18 generally recites a method for operating a secure operations center comprising providing information (in the form of records) about customers and events on the network. As summarized above, Petitioner sufficiently shows that “Duvall-Chu-Cogger's residue data-review system, like Cogger's CSM, provides ‘a secure operations center as part of a security monitoring system for a customer computer network.’” Pet. 68.

Regarding Patent Owner's arguments as to how to combine Cogger, Petitioner sufficiently shows that “Cogger's CSM would be implemented as part of Duvall-Chu's network-administrator resolution pathway for receiving and analyzing tickets transmitted from subscriber networks.” *Id.* (citing Ex. 1003 ¶ 230; Pet. § VI.D.1). And as noted above, Petitioner describes

IPR2023-00889

Patent 7,895,641 B2

implementing Cogger's ticket teachings with Duvall-Chu's network administration system. Petitioner's showing is sufficient on this preliminary record.

Moreover, Petitioner need not bodily incorporate Cogger's ticket system into Duvall-Chu's filter processing and management system for purposes of obviousness to satisfy what Patent Owner describes as an alleged "remote management" system. To the extent a "secure operations center" as recited in the preamble of claim 18 implicates a remote management system, Patent Owner will have the opportunity to tie its arguments clearly to claim limitations during trial. To the extent claim 18 or Petitioner's showing somehow implicates a "remote management" system, Petitioner sufficiently supports the showing, wherein the Duvall-Chu combination sends tickets from analysts at corporate network computers to expert analysts at Cogger's CSM for optimizing and providing uniform security resolution and tracking across the network. *See* Pet. 64–67.

Finally, claim 18 is a broad claim and does not require the claimed security analyst to resolve any network problems. Rather, claim 18 recites "providing the problem ticket to a security analyst console for analysis," which requires a capability for analysis and/or amounts to an intended use of the console, without specifying any particular analysis. As Petitioner sufficiently shows with respect to claims 1 and 18, Duvall's and Chu's system already provide information and feedback about security issues on a network to trained network analysts/users as part of an "analyst system," as outlined above in connection with claim 1. *See, e.g.,* Pet. 40–42 (addressing feedback in Duvall), 67 ("Chu, for example, already discloses alerting a user with expertise to resolve residue data." (citing Ex. 1005, 44)); Ex. 1004, 5:62–65 (providing feedback to a user's screen). Petitioner also sufficiently

IPR2023-00889

Patent 7,895,641 B2

shows (for purposes of institution) that Cogger teaches a “problem ticket” submitted to the CSM and that a person of ordinary skill in the art “would have been motivated to provide a similar ‘analyst console’ to analysts operating Duval-Chu-Cogger’s service to analyze event information received in a trouble ticket and update filters as appropriate.” Pet. 74 (citing Ex. 1033, 2:24–30, 3:65–67; Ex. 1003 ¶ 244).

Based on the foregoing discussion and preliminary record, we determine that Petitioner demonstrates a reasonable likelihood of showing that claim 18 would have been obvious.

Turning to dependent claims 19–25, having reviewed Petitioner’s arguments and supporting evidence in this preliminary record, including the arguments summarized above for claim 1, we determine Petitioner sufficiently shows for purposes of this Decision that the combination of Duvall, Chu, and Cogger would have rendered these claims 19–25 obvious. *See* Pet. 75–85. Patent Owner does not address Petitioner’s showing with respect to these claims. *See generally* Prelim. Resp. Based on the preliminary record, we determine Petitioner demonstrates a reasonable likelihood of showing that claims 19–25 would have been obvious.

IV. CONCLUSION

After considering the evidence and arguments of record, we determine that Petitioner has demonstrated a reasonable likelihood of success with respect to at least one of the challenged claims. Accordingly, an *inter partes* review of all of the claims is hereby instituted on the ground presented in the Petition. *See* 37 C.F.R. § 42.108(a).

At this stage of the proceeding, the Board has not made a final determination as to the patentability of any challenged claims or any

IPR2023-00889

Patent 7,895,641 B2

underlying factual or legal issues. The final determination will be based on the record as developed during the *inter partes* review.

V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of the challenged claims of the '641 patent is instituted with respect to the grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '641 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

IPR2023-00889

Patent 7,895,641 B2

PETITIONER:

Jonathan Tuminaro

Dan Block

Michael Specht

Steven Pappas

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

jtuminar-ptab@sternekessler.com

dblock-ptab@sternekessler.com

mspecht-ptab@sternekessler.com

spappas-ptab@sternekessler.com

PATENT OWNER:

Nolan M. Goldberg

Baldassare Vinti

PROSKAUER ROSE LLP

NGoldbergPTABMatters@proskauer.com

BVinti@proskauer.com

Jonathan A. Roberts

Raymond Y. Mah

Joseph A. Rhoa

NIXON & VANDERHYE P.C.

jr@nixonvan.com

rym@nixonvan.com

jar@nixonvan.com

EXHIBIT 2

Trials@uspto.gov
571-272-7822

Paper: 9
Entered: November 17, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

BT AMERICAS INC.,
Patent Owner.

IPR2023-00888
Patent 7,159,237 B2

Before KARL D. EASTHOM, GEORGIANNA W. BRADEN, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

BRADEN, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

IPR2023-00888

Patent 7,159,237 B2

I. INTRODUCTION

Palo Alto Networks, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–42 (the “challenged claims”) of U.S. Patent No. 7,159,237 B2 (Ex. 1001, “the ’237 patent”). Paper 2 (“Pet.”). BT Americas Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). With our permission (Ex. 3001), Petitioner filed a Reply, to address claim construction arguments. Paper 7 (“Reply”). Patent Owner filed a Sur-reply. Paper 8 (“Sur-reply”).

We have authority to determine whether to institute an *inter partes* review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4. An *inter partes* review may not be instituted unless it is determined that “the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314; *see also* 37 C.F.R. § 42.4(a) (2022) (“The Board institutes the trial on behalf of the Director.”). The reasonable likelihood standard is “a higher standard than mere notice pleading,” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

For the reasons provided below and based on the record before us, we determine Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. Accordingly, we decline to institute *inter partes* review on any of the alleged grounds of unpatentability.

IPR2023-00888

Patent 7,159,237 B2

II. BACKGROUND

A. Real Parties in Interest

Petitioner identifies only itself as real party in interest. Pet. 3. Patent Owner identifies itself and British Telecommunications plc as real parties in interest. Paper 4 (Patent Owner’s Mandatory Notices), 1.

B. Related Proceedings

The parties identify the following district court cases involving the ’237 patent: *British Telecommunications PLC v. Fortinet, Inc.*, 1:18-cv-01018-CFC-MPT (D. Del.) and *British Telecommunications PLC and BT Americas, Inc. v. Palo Alto Networks, Inc.*, 1:22-cv-01538 (D. Del.). Pet. 3; Paper 4, 1. The parties also identify *inter partes* review proceeding IPR2019-01325. *Id.*

Patent Owner further identifies *inter partes* review proceedings IPR2019-01324 and IPR2023-00889 before the Board as related matters. Paper 4, 1.

C. The ’237 Patent (Ex. 1001)

The ’237 patent is titled “Method and System for Dynamic Network Intrusion Monitoring, Detection and Response,” and issued on January 2, 2007. Ex. 1001, codes (45), (54).

1. Written Description

The ’237 patent relates to “network security and, more specifically, to methods and systems for dynamic network intrusion monitoring, detection and response.” Ex. 1001, 1:7–9. More specifically, the ’237 patent discloses “a managed security monitoring service (the ‘MSM service’) that monitors a customer’s network activity using a probe or ‘sentry’ system, collects status data from monitored components, filters or otherwise analyzes the collected

IPR2023-00888

Patent 7,159,237 B2

data for activity possibly implicating security concerns, alerts and transmits information about such activity to trained security analysts working at secure operations centers (‘SOCs’), and then guides the security analysts and customer through an appropriate response (with appropriate follow-up, if necessary).” *Id.* at 1:50–59.

Figure 1 of the ’237 patent reproduced below:

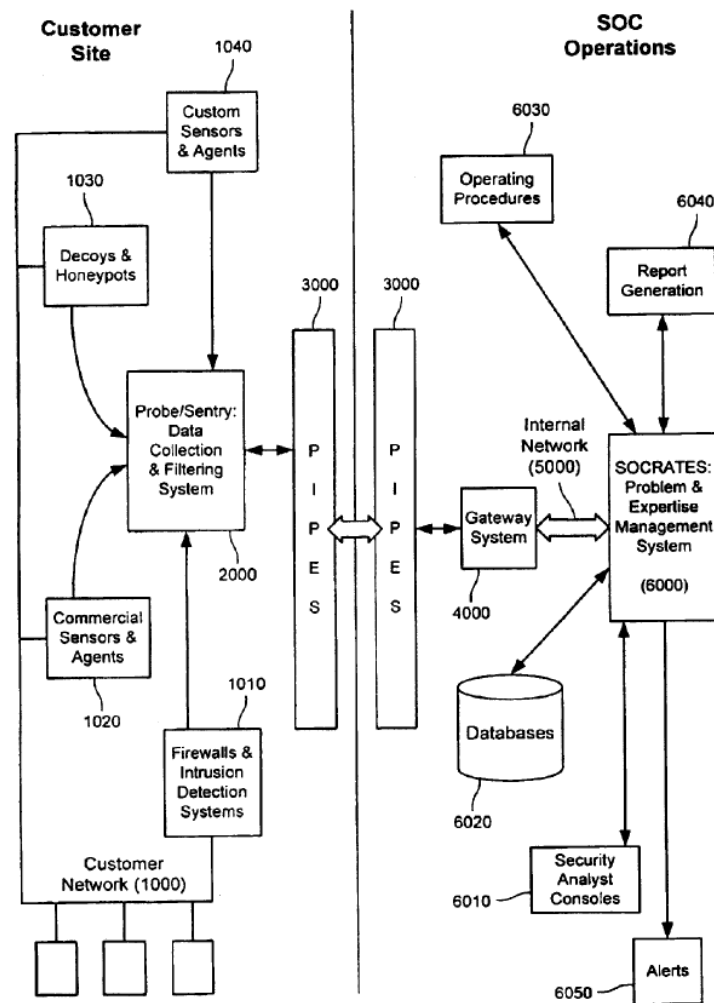


FIG. 1

Id. at Fig. 1. Figure 1 is a diagram depicting “an overview of the system architecture of an exemplary embodiment” disclosed in the ’237 patent. *Id.* at 3:60–61. Figure 1 is divided into two portions, components and systems that operate on the customer site (that is, within the customer’s firewall) and

IPR2023-00888

Patent 7,159,237 B2

components and systems that operate within the SOC (that is, within the SOC firewall). *Id.* at 4:38–42. Pipes 3000 provides an encrypted, secure communications path and message protocol for messages sent back and forth between probe/sentry system 2000 at the customer site and gateway system 4000 at the SOC. *Id.* at 5:44–48.

Probe/sentry system 2000 monitors sensors attached to customer network 1000 for evidence of potential security-related events happening on network 1000. *Id.* at 4:48–52. The sensors can include firewalls and intrusion detection systems 1010, commercially available sensors and agents 1020, decoys and honeypots 1030, and custom sensors and agents 1040. *Id.* at 4:52–57. Probe/sentry system 2000 can monitor and collect information from any network component that can be configured to provide a status data (including audit log data and other audit information) concerning the status of network 1000 and its components. *Id.* at 4:58–63.

Figure 2 of the '237 patent is reproduced below:

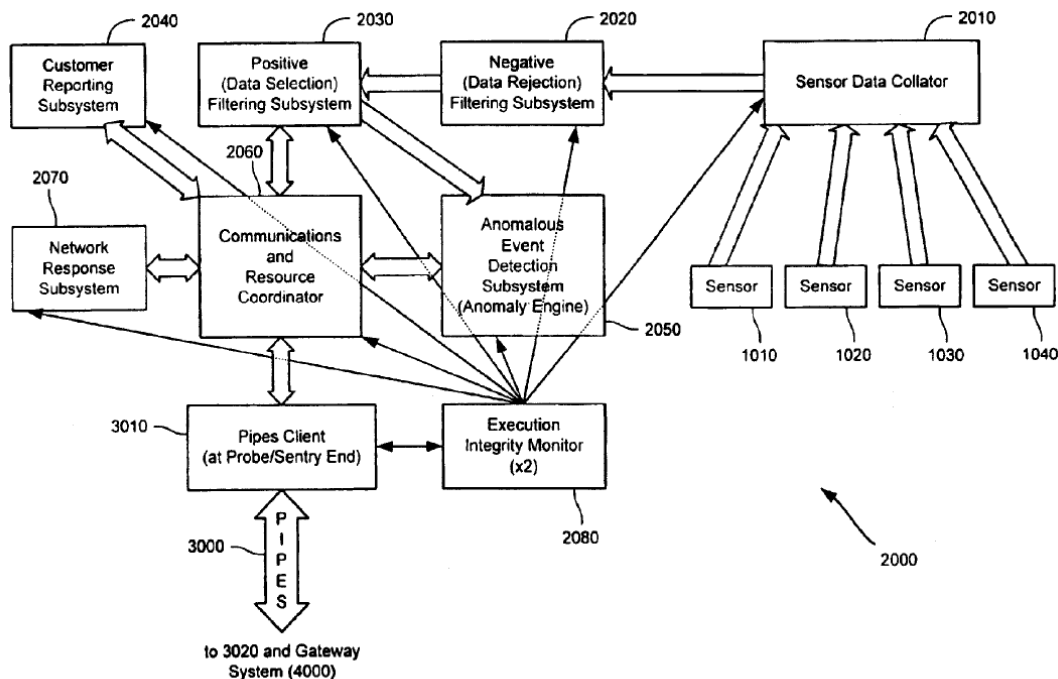


FIG. 2

IPR2023-00888

Patent 7,159,237 B2

Figure 2 is a diagram depicting “a system overview of an exemplary embodiment of a probe/sentry system in an exemplary embodiment” disclosed in the ’237 patent. *Id.* at 3:62–64. According to the ’237 patent, “[d]ata collected by sensors 1010, 1020, 1030 and 1040 are collated by sensor data collator 2010.” *Id.* at 8:41–45. “Once collated, the data is first filtered by negative filtering subsystem 2020, which discards uninteresting information, and then by positive filtering subsystem 2030, which selects possibly interesting information and forwards it to communications and resource coordinator 2060.” *Id.* at 8:45–50. “Data neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030 form the ‘residue,’ which is sent to anomaly engine 2050 for further analysis.” *Id.* at 8:50–53. “Anomaly engine 2050 determines what residue information may be worthy of additional analysis and sends such information to communications and resource coordinator 2060 for forwarding to the SOC.” *Id.* at 8:53–57. “Communications and resource coordinator 2060 creates sentry messages out of the interesting status data and forwards those messages on to gateway system 4000.” *Id.* at 8:60–62.

The ’237 patent further discloses a Secure Operations Center Responsive Analyst Technical Expertise System (“SOCRATES”). *Id.* at 3:55. According to the ’237 patent, “[t]he SOCRATES system is a consolidated system used to manage customers’ problems and the supporting data helpful in resolving such problems.” *Id.* at 9:50–52. The SOCRATES system “provides security analysts at a SOC a single, integrated system with which to track information concerning, for example, problems, companies, people, contacts, tools, and installed network components and known vulnerabilities.” *Id.* at 9:52–56.

IPR2023-00888

Patent 7,159,237 B2

In another embodiment, the managed security monitoring service allows for customization and complex data analysis. *Id.* at 2:21–22. For example, the service may be customized, either dynamically or offline, to accommodate network-specific needs and to reflect feedback received about the demonstrated efficacy of a real-world response to an actual event. *Id.* at 2:23–26. The '237 patent discloses that status data collected, filtered, or otherwise analyzed by probe/sentry system 2000 can either remain in the customer's hands or be provided to service personnel for further analysis (e.g., cross-customer analysis). *Id.* at 5:19–26. According to the '237 patent, in a preferred embodiment, the software and filters of probe/sentry system 2000, may be adaptive or, alternatively, may be manually updated offline or dynamically (that is, during actual operation). *Id.* at 5:26–29. The '237 explains that, updates can be sent from the SOC to the probe/sentry system and signed, verified and then securely installed. *Id.* at 5:30–32.

2. *Illustrative Claims*

As noted previously, Petitioner challenges claims 1–42 of the '237 patent, of which claims 1, 18, and 26 are independent. Pet. 1; Ex. 1001, 35:38–38:47. Claim 1 is illustrative of the challenged subject matter and is reproduced below.

1. A method of operating a probe as part of a security monitoring system for a computer network, comprising:
 - a) collecting status data from at least one monitored component of said network;
 - b) analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
 - c) transmitting information about said identified events to an analyst associated with said security monitoring system;

IPR2023-00888

Patent 7,159,237 B2

- d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and
- e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

Ex. 1001, 35:39–57.

D. Asserted Challenges to Patentability and Evidence of Record

Petitioner challenges the patentability of claims 1–42 of the '237

patent based on the following reference or combination of references:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–7, 15–23, 26–32, 40–42	103 ¹	Duvall ² , Chu ³
7–13, 16, 24, 32–38, 41	103	Duvall, Chu, Trcka ⁴
14–15, 25, 39–40	103	Duvall, Chu, Trcka, Ziese ⁵

In support of its patentability challenge, Petitioner relies on, *inter alia*, the Declaration of Kevin Jeffay, Ph.D. (“Dr. Jeffay”). Ex. 1003. In support of its Preliminary Response, Patent Owner relies on, *inter alia*, the Declaration of Wenke Lee, Ph.D. (“Dr. Lee”). Ex. 2001.

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), included revisions to 35 U.S.C. § 103 that became effective as of March 16, 2013. The application for the '237 patent was filed before March 16, 2013. Ex. 1001, code (22). Accordingly, for purposes of institution, we apply the pre-AIA version of 35 U.S.C. § 103.

² US Patent 5,884,033, issued Mar. 16, 1999; filed May 15, 1996 (“Duvall,” Ex. 1004).

³ Yang-hua Chu, *Trust Management for the World Wide Web*, M.I.T. (June 13, 1997) (“Chu,” Ex. 1005).

⁴ US Patent Application Publication No. 2001/0039579 A1, published Nov. 8, 2001 (“Trcka,” Ex. 1014).

⁵ US Patent 6,484,315 B1, issued Nov. 19, 2002; filed Feb. 1, 1999 (“Ziese,” Ex. 1015).

IPR2023-00888

Patent 7,159,237 B2

III. PRELIMINARY MATTERS

A. Claim Construction

A claim “shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b).” 37 C.F.R. § 42.100(b). Under that standard, the “words of a claim ‘are generally given their ordinary and customary meaning.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).

Petitioner asserts that “no claim terms require an explicit construction” and that “the challenged claims are unpatentable under either the ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention in light of the specification and the prosecution history, or the district court’s previous claim constructions. Pet. 14.

Petitioner acknowledges that the limitation “post-filtering residue is data neither discarded nor selected by filtering” in independent claims 1, 18, and 26 was construed in a district court case to which it was not a party. Pet. 33. According to Petitioner, the parties in the that district court case agreed that limitation should be construed as “status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering.” *Id.* (citing Ex. 1013, 4). Petitioner contends that “under either this agreed-upon construction or the claim’s plain language, Duvall teaches” the limitation. *Id.* (citing Ex. 1003 ¶ 125); *see also* Pet. 35 (citing Ex. 1003 ¶ 130; Ex. 1004, 4:27–30, 4:65–5:7).

Patent Owner asserts that “post-filtering residue” has been misconstrued and misapplied by Petitioner. Prelim. Resp. 28–32. According to Patent Owner, Petitioner’s implicit construction of the

IPR2023-00888

Patent 7,159,237 B2

limitation suggests “that the ‘plain language of this element does not require any data to actually be ‘discarded’ or ‘selected by filtering’—only that the ‘post-filtering residue is data neither discarded nor selected by filtering.’” *Id.* at 30. Patent Owner contends Petitioner omits the requirement that the “residue” be “post-filtering” and impermissibly broadens the residue to include (1) any data, not just status data, and (2) in-flight or mid-filtering data—that is, data that is still in the process of being filtered. *Id.* at 30–31. Patent Owner admits that the IP addresses used in the Duvall references are status data, but then argues that “Petitioner bears the burden to show how Duvall actually analyzes any leftover status data to identify potentially security related events.” *Id.* at 31.

We agree with Patent Owner that limitation b) requires a filtering process that produces the claimed residue from the filtering, followed by an analysis of the post-filtering residue. We also agree that the filtering and analysis is performed on status data. Nonetheless, as discussed in detail below, we find Duvall teaches the disputed limitation even under Patent Owner’s construction.

We do not construe any other limitations or terms of the challenged claims because construction is needed only for those terms “that are in controversy, and only to the extent necessary to resolve the controversy.” *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Principles of Law Regarding Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

IPR2023-00888

Patent 7,159,237 B2

invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-obviousness.⁶ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result is considered in the ultimate determination of obviousness. *Id.* at 416–417.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic Inc. v. Avid Tech.*,

⁶ Patent Owner states that it raised arguments regarding indicia of non-obviousness in response to a prior petition challenging the ’237 patent but that Petitioner failed to address those considerations in its Petition. Prelim. Resp. 12–13 (citing *Robert Bosch Tool Corp. v. SD3, LLC*, IPR2016-01753, Paper 15 at 28 (PTAB Mar. 22, 2017)). We note that the decision cited by Patent Owner, *Robert Bosch Tool*, denied institution where, amongst other things, a Petitioner failed to discuss indicia of non-obviousness in its Petition despite having such evidence in a related ITC proceeding where Petitioner was a party. That is not the case here. In the present case, the only previously filed Board proceeding (1) does not involve Petitioner and (2) does not have readily identifiable indicia of non-obviousness. Specifically, in the present Preliminary Response, Patent Owner does not cite where in its prior Preliminary Response the indicia of non-obviousness may be found, nor does Patent Owner introduce sufficient evidence regarding objective indicia of non-obvious at this stage in the proceeding. Thus, Patent Owner’s arguments are accorded no weight in our analysis.

IPR2023-00888

Patent 7,159,237 B2

Inc., 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b). The burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation marks omitted). Furthermore, the prior art itself can reflect the appropriate level of ordinary skill in the art. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Here, Petitioner asserts a person of ordinary skill in the art at the time of the ’237 patent, “would have had a B.S. degree in Computer Science, Computer Engineering, or an equivalent field, as well as at least 2–3 years of academic or industry experience in the design, analysis, and monitoring of computer networks, including issues of network security and network administration, or comparable industry experience.” Pet. 12 (citing Ex. 1003 ¶¶ 61–62).

Patent Owner does not assert a different level of skill in the art at the time of the alleged invention at this time. Prelim. Resp. 28.

For the purposes of this Decision, we adopt Petitioner’s level of ordinary skill in the art because it appears consistent with the problems addressed in the ’237 Patent and the prior art of record, except that we

IPR2023-00888

Patent 7,159,237 B2

delete the qualifier “at least” in the phrase “at least 2–3 years” to eliminate vagueness as to the stated amount of academic or industry experience.

D. Overview of Asserted Prior Art of Record

1. Duvall (Ex. 1004)

Duvall is a U.S. Patent, issued March 16, 1999, titled “Internet Filtering System for Filtering Data Transferred over the Internet Utilizing Immediate and Deferred Filtering Actions.” Ex. 1004, codes (19), (45), (54). Duvall relates to “filtering messages transmitted between the Internet and a client computer.” *Id.* at 1:7–8. Duvall discloses a client-based filtering system compares portions of incoming and/or outgoing messages with filtering information stored in a filter database. and determines whether to block or allow the incoming and/or outgoing transmissions of messages in response to the comparison. *Id.* at 1:31–35. Duvall explains that in response to a match between certain information in portions of the message and the filtering information, the system can employ one of a number of different specified blocking options, including discarding incoming data, preventing execution of an open command. or replacing parts of received data. *Id.* at 1:35–40.

One embodiment of Duvall is shown in Figure 1, reproduced below:

IPR2023-00888

Patent 7,159,237 B2

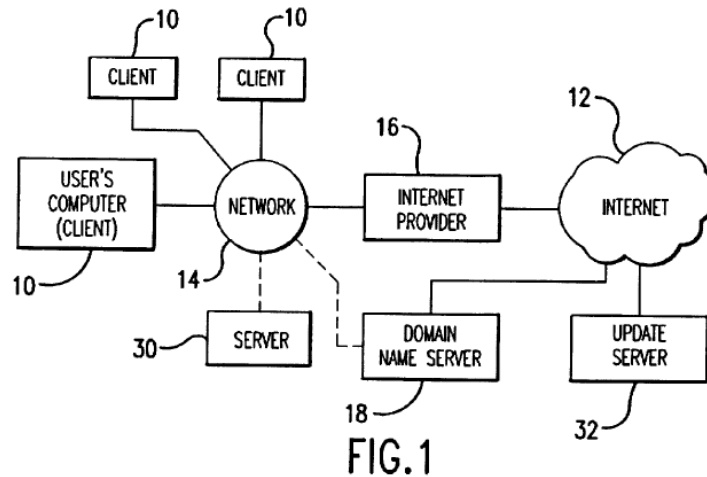
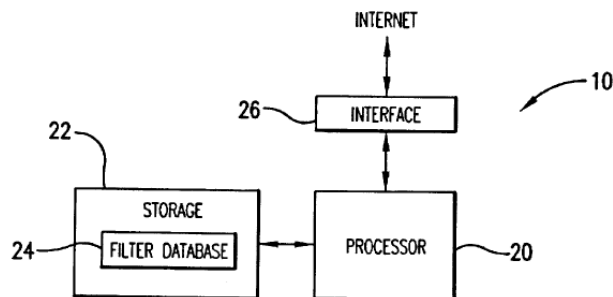


Figure 1 depicts “a block diagram of a network with a client computer for accessing the Internet.” *Id.* at 2:24–25. The network includes a user with a computer that serves as client computer 10 that communicates with other computers over Internet 12.” *Id.* at 2:34–35. According to Internet Protocol version 4, each computer on or connected to the Internet has an IP address that identifies the location of the computer. *Id.* at 2:51–53. Duvall’s filter system can filter messages on the basis of IP address. *Id.* at 4:5–11, 4:37–39.

Another embodiment of Duvall is shown in Figure 2, reproduced below:



IPR2023-00888

Patent 7,159,237 B2

Figure 2 depicts a block diagram of client computer 10 with a filtering system. *Id.* at 2:26–27. In this embodiment, as shown in Figure 2, “a filtering system resides in client computer 10.” *Id.* at 3:43–44. “Processing by the filtering system is carried out by the computer’s processor 20. and the system uses the computer’s storage 22 to store a filter database 24.” *Id.* at 3:44–46. Duvall also discloses an embodiment in which “the filtering system can be provided from a server 30 that is on the client’s own network 40.” *Id.* at 8:18–21. “This version of the filtering system uses the same type of filter database as a client-based filtering system, but the filter database is located on server 30.” *Id.* at 8:23–26.

Duvall discloses a “filter database [that] has lists of filters, some of which are identified as either ALLOW filters or BLOCK filters for respectively allowing or blocking transmission.” *Id.* at 3:64–66. “Each filter entry in the filter database also has a field for specifying an action to be taken by the client if that filter were retrieved.” *Id.* at 4:12–14. “These actions are essentially divided into two groups, direct action or deferred action.” *Id.* at 4:14–15. “Direct actions indicate that the system should unconditionally allow or unconditionally block the transmission.” *Id.* at 4:15–17. “If . . . it is determined that no immediate action must be taken, it is determined whether a deferred action must be taken.” *Id.* at 4:65–67. Additionally, a filter can indicate that a deferred action should be taken. *Id.* at 4:65–5:1; 6:19–20.

Duvall discloses filters “stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last.” *Id.* at 4:27–29. Duvall further discloses, “[i]f there is no deferred action, the system can default to allow the transmission . . . , or it can default to block the transmission.” *Id.* at 5:1–3. Deferred filter entries preferably have

IPR2023-00888

Patent 7,159,237 B2

additional fields, including fields for (1) a keyword, typically a command such as GET; (2) a filter pattern to be compared to data in the message, typically a string of characters; (3) a directional indicator (IN/OUT) for indicating incoming or outgoing transmissions; (4) a compare directive for the type of match; and (5) an action to be taken, typically to allow or block the transmission. *Id.* at 5:8–15.

2. *Chu (Ex. 1005)*

Chu is a Master's thesis titled "Trust Management for the World Wide Web" submitted to the Massachusetts Institute of Technology Department of Electrical Engineering and Computer Science. Ex. 1005, 3.

Chu relates to "trust management . . . in the context of the World Wide Web. *Id.* For example, *Chu* discloses sample policies addressing the question of "should I download the active content at this URL." *Id.* 43–48. *Chu* discloses policies that employ a "blacklist" and a "whitelist." *Id.* at 44. The blacklist is a list of sites or directories the computer should not download codes from. *Id.* According to *Chu*, the use of such lists "can be very effective in practice . . . [because] Firewall vendors can compile a blacklist of Web sites that serve potentially dangerous active codes, and place the list in clients' firewalls." *Id.* *Chu* states that "[t]he blacklist and whitelist ensure good automation of the trust decision process if the lists are reasonably complete." *Id.* If the request URL is neither in the blacklist nor the white list, then *Chu* discloses that the system can return the term "unknown."

One embodiment of *Chu* is reproduced below:

Policy in English

Do not download the code if the URL is served from Harvard or CalTech Web servers. Download it automatically if served from MIT. Prompt me for my attention otherwise.
--

IPR2023-00888

Patent 7,159,237 B2

As shown above, Chu directs the system to send the user an attention prompt in that case and states “[u]ser intervention is needed only when the given URL is in neither the blacklist nor the whitelist.” *Id.*

3. *Trcka (Ex. 1014)*

Trcka is a U.S. Patent Application Publication, published on November 8, 2001, titled “Network Security and Surveillance System.” Ex. 1014, codes (12), (43), (54).

Trcka relates to “[a] network security and surveillance system [that] passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic.” Ex. 1014, code 57. According to Trcka, “[a] set of analysis applications and other software routines allows authorized users to interactively analyze the low-level traffic recordings to evaluate network attacks, internal and external security breaches, network problems, and other types of network events.” *Id.*

Trcka discloses “analysis applications [that] can . . . be used to view, analyze and process . . . traffic data,” including “functionality for performing such actions as displaying user-specified types of network events, conducting pattern searches of selected packet data, reconstructing transaction sequences, and identifying pre-defined network problems.”

Id. ¶ 16. Trcka also discloses “analysis tools . . . for allowing authorized users to perform interactive, off-line analyses of recorded traffic data.”

Id. ¶ 53. Trcka discloses a “graphical user interface (GUI)” through which “the user can launch and control the various analysis applications . . . through a common set of menus and controls.” *Id.* ¶ 79.

IPR2023-00888

Patent 7,159,237 B2

4. *Ziese (Ex. 1015)*

Ziese is a U.S. Patent, issued November 19, 2002, titled “Method and System for Dynamically Distributing Updates in a Network.” Ex. 1015, codes (12), (45), (54). Ziese discloses “dynamically distributing intrusion detection and other types of updates in a network that substantially eliminate or reduce disadvantages and problems associated with prior methods and systems.” *Id.* at 2:2–6. According to Ziese, “programs are automatically updated by downloading and distributing an update in response to an automated event,” and “[a]s a result, systems with a common program separately running at several sites may update each site with no or minimal operator interaction.” *Id.* at 2:39–44.

IV. ANALYSIS

A. *Alleged Obviousness of Claims 1–7, 15–23, 26–32, and 40–42 in view of Duvall and Chu*

Petitioner contends claims 1–7, 15–23, 26–32, and 40–42 would have been obvious to a person of ordinary skill in the art in view of the combined teachings of Duvall and Chu. Pet. 14–59. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 32–64. For the reasons discussed below, at this stage of the proceeding, we are not persuaded that Petitioner has established a reasonable likelihood of success on this challenge.

1. *Analysis of Independent Claim 1*

a) *“A method of operating a probe as part of a security monitoring system for a computer network”*

Petitioner contends that Duvall discloses a “*a security monitoring system for a computer network*,” because Duvall is directed to “filtering messages transmitted between the Internet and a client computer” to ensure content that implicates security concerns does not reach recipients. Pet. 25

IPR2023-00888

Patent 7,159,237 B2

(citing Ex. 1004, 1:7–24, 1:12–20, 1:27–29; Ex. 1003 ¶ 113). According to Petitioner, “Duvall’s filtering system monitors transmissions for questionable content that should be blocked.” *Id.* (citing Ex. 1004, 3:33–37, 5:8–15, 6:10–42; Ex. 1003 ¶ 115). Petitioner argues that a person of ordinary skill in the art “would have been motivated to block content that may have carried viruses or malware” and that “no modifications would be needed in Duvall’s system—domains (e.g., URLs or IP addresses) believed to carry security-implicating content (e.g., viruses) would simply be included in Duvall’s blocking filters.” *Id.* at 26 (citing Ex. 1004, 6:10–27; Ex. 1003 ¶ 115).

Petitioner further contends that Duvall’s server 30 is a probe that provides a filtering system. Pet. 26–27 (citing Ex. 1004, 8:18–21, 1:60–64, Fig. 1; Ex. 1013 ¶ 2). According to Petitioner, “Duvall’s server 30 collects and analyzes data from other network components to which it is attached, such as clients 10” and that its “filtering system may be part of a firewall.” *Id.* at 27–28 (citing Ex. 1004, 1:59–64, 8:21–223).

Patent Owner has not provided any arguments regarding this specific claim limitation and the application of Duvall and Chu. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

“Whether to treat a preamble term as a claim limitation is determined on the facts of each case in light of the claim as a whole and the invention described in the patent.” *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358 (Fed. Cir. 2010) (internal quotation marks omitted). “Absent clear reliance on the preamble in the prosecution history, or in situations where it is necessary to provide antecedent basis for the body of the claim, the preamble generally is not limiting.” *Symantec Corp. v. Computer Assocs.*

IPR2023-00888

Patent 7,159,237 B2

Int'l, Inc., 522 F.3d 1279, 1288 (Fed. Cir. 2008) (internal quotation marks and citation omitted). Additionally, preamble language that merely states the purpose or intended use of an invention generally is not treated as limiting the scope of a claim. See *Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp.*, 320 F.3d 1339, 1345 (Fed. Cir. 2003); *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir. 1997). Yet, when the limitations in the body of the claim rely upon or derive essential structure from the preamble, then the preamble acts as a necessary component of the claimed invention and is limiting. See *Eaton Corp. v. Rockwell Int'l Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003).

Our reviewing court has explained, however, that a “conclusion that some preamble language is limiting does not imply that other preamble language, or the entire preamble, is limiting.” *Cochlear Bone Anchored Sols. AB v. Oticon Med. AB*, 958 F.3d 1348, 1355 (Fed. Cir. 2020); see *TomTom, Inc. v. Adolph*, 790 F.3d 1315, 1322-23 (Fed. Cir. 2015) (holding the court erred in determining that it had to construe the entire preamble if it construed a portion of it), citing *Loctite Corp. v. Ultraseal Ltd.*, 781 F.2d 861, 868 (Fed. Cir. 1985), *overruled in part on other grounds by Nobelpharma AB v. Implant Innovations, Inc.*, 141 F.3d 1059, 1068 (Fed. Cir. 1998) (en banc in part). The Court in *Cochlear Bone Anchored* specifically held that even when a phrase in a preamble provides a necessary structure for a claim, that preamble structure does not necessarily convert the entire preamble into a limitation, particularly one that only states the intended use of the invention. 958 F.3d at 1355.

Based on the current record, we find at least part of the preamble limiting because (1) the claim limitation relating to “probe,” relies on the preamble for antecedent basis. Accordingly, we find at least this portion of

IPR2023-00888

Patent 7,159,237 B2

the preamble recites an essential structure of the security monitoring system and is limiting. We need not reach a determination on whether the entirety of the preamble is limiting because at this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render the preamble obvious to a person of ordinary skill in the art at the critical time.

b) “collecting status data from at least one monitored component of said network”

Petitioner contends that meets this limitation because Duvall’s server 30 analyzes (i.e., monitors) data received from clients 10, which reside on the same network. Pet. 28. Specifically, Petitioner argues Duvall’s filtering system, which is on a client’s own network server, compares the IP address from a transmitted message to determine if some action is needed. *Id.* at 29 (citing Ex. 1004, 4:22–27, 2:35–37, 2:42–44). According to Petitioner, the IP address of a message is “status data” because it is data extracted from network traffic and provides the status of the network and its component. *Id.* at 30 (citing Ex. 1004, 4:39–42, 5:66–6:27; Ex. 1013 ¶ 119).

Other than agreeing that IP addresses are status data, Patent Owner has not provided any arguments regarding this specific claim limitation and the application of Duvall and Chu. Prelim. Resp. 31. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time. Specifically, we are satisfied because IP addresses are status data and

IPR2023-00888

Patent 7,159,237 B2

Duvall's monitors transmitted messages on client 10 and then compares the IP address from a transmitted message to determine if some action is needed. *See* Ex. 1004, 4:22–27, 2:35–37, 2:42–44.

c) *“analyzing status data to identify potentially security-related events represented in the status data”*

Petitioner contends that Duvall meets the claim limitation because Duvall discloses filtering based on IP address (i.e., “status data”) and other information: “[w]hen a message is transmitted, whether that message is incoming or outgoing with respect to the client computer, the filtering system compares the IP address and/or other information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken.” Pet. 31 (citing Ex. 1004, 4:22–27).

Petitioner further contends that Duvall teaches “identify[ing] potentially security-related events” because the purpose of Duvall’s deferred filtering analysis is to identify threats that do not match Duvall’s initial “ALLOW or BLOCK filters”—i.e., unknown threats. Reply 3 (citing Pet. 17–19; Ex. 1003 ¶¶ 99–101). According to Petitioner “[k]nown threats would have been blocked at this initial step while permitted data would have been allowed.” *Id.* Petition argues that Duvall’s deferred action step analyzes any residual data to identify any potential threats that were not originally blocked by the BLOCK filters—i.e., unknown threats. *Id.* (citing Ex. 1004, 5:8–19, 6:19–41 (identifying transmissions to/from sources that include “a potentially objectionable phrase” such as “sex” or “xxx”); Pet. 18–19; Ex. 1003 ¶¶ 100–101). Petitioner further argues that the ’237 patent does not limit the scope of what may be considered “security-related,” because the ’237 patent states that “the present invention is usable generally

IPR2023-00888

Patent 7,159,237 B2

for [] monitoring of any system.” *Id.* at 4 (citing Ex. 1001, 15:63–16:5; Pet. 9).

Patent Owner disputes Petitioner’s interpretation of the claim and disputes that Duvall and Chu analysis post-filtered status data to identify a potentially security-related event. Prelim. Resp. 34–37. According to Patent Owner, Duvall and Chu only teach filtering for things that are already known, but “[n]either of them analyzes any data to identify *potential* threats after filtering (*i.e.*, previously unknown threats from the post-filtering residue).” *Id.* at 34. Patent Owner argues that subjectively objectionable material is different than an objectively identified security-related event. *Id.*; *see also* Sur-Reply 4 (“[O]bjectionable material’ is different from ‘security related’ material.”).

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time. Specifically, we are satisfied because the term “potentially security-related events” is broad enough to encompass the objectionable material disclosed in Duvall and/or the black list sites of Chu. Specifically, we credit the testimony of Dr. Jeffay, who explains that Duvall’s and Chu’s techniques apply to other security-related contexts, and that objectionable material also presents virus- and malware-related risks. *See* Ex. 1003 ¶¶ 113–14, 134. Patent Owner attempts to unreasonably limits claims with arguments that are not commiserate with the scope of the claims as issued.

IPR2023-00888

Patent 7,159,237 B2

d) wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering”

Petitioner contends that Duvall meets the claim limitation because Duvall uses “direct action” filters on all transmissions to indicate whether the system should allow or block a transmission. Pet. 30–31 (citing Ex. 1004, 4:12–21, 5:8–29; Ex. 1013 ¶ 119). Petitioner argues that Duvall’s “filter database has lists of filters, some of which are identified as either ALLOW filters or BLOCK filters for respectively allowing or blocking transmission.” *Id.* at 31 (citing Ex. 1004, 3:64–66). According to Petitioner, “[e]ach filter entry in the filter database [] has a field for specifying an action to be taken by the client if that filter were retrieved,” and “[t]hese actions are essentially divided into two groups, direct action or deferred action.” *Id.* at 31–32 (citing Ex. 1004, 4:12–15). Petitioner notes that Duvall’s filters are implemented in sequence as they “‘are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last,’ where the ‘ALLOW’ and ‘BLOCK’ filters are direct action filters.” *Id.* at 32–33 (citing Ex. 1004, 4:27–30; Ex. 1003 ¶¶ 122–123). Petitioner argues that if immediate action is not required by the filters, then what is left is “residue data” that is passed for further analysis by Duvall’s deferred action filters. *Id.* at 35 (citing Ex. 1004, 4:27–30, 4:65–5:7).

Petitioner further contends that such “data allowing and blocking comprises ‘positive filtering’ and ‘negative filtering’ in accordance with the” claim construction that Patent Owner agreed to in a district court litigation where the ’237 patent was asserted previously. *Id.* at 35 (citing Ex. 1003 ¶¶ 126–129). Petitioner argues that the district court’s claim construction does mean that “the ‘residue’ cannot be subject to further filtering as part of

IPR2023-00888

Patent 7,159,237 B2

the analysis, as long as that analysis occurs *after* (i.e., ‘post’) the negative and positive filtering. Reply 1. And, according to Petitioner, the ’237 patent describes performing stages of “negative filtering” and “positive filtering,” followed by further analysis by an “anomaly engine,” but the type of analysis performs in limited or restricted—only that the “anomaly engine” “determines what residue information may be worthy of additional analysis,” which may include additional filtering. *Id.* at 2 (citing Ex. 1001, 8:45–57). Thus, Petitioner concludes that Duvall’s IP addresses are residue status data “that underwent negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering—i.e., ‘post-filtering residue,’” and therefore, meet the claim limitation. Pet. 35–36 (citing Ex. 1003 ¶ 130).

Patent Owner disputes Petitioner’s interpretation of the claim and disputes that Duvall meets the claim limitation. Prelim. Resp. 29–31. Patent Owner first acknowledges the claim construction used in the district court litigation where “post-filtering residue, wherein the postfiltering residue is data neither discarded nor selected by filtering” was construed to mean “status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering.” *Id.* at 29 (citing Ex. 1013, 4). Then, Patent Owner contends that Duvall does not create “post-filtering residue” because Duvall does not analyze status data after all filtering is completed. *Id.* at 30–31. Rather, according to Patent Owner, “the filtering process must be distinct from the analysis that follows the filtering” and that Petitioner’s use of “in-fight” or mid-filtered data is still in the process of being filtered and therefore would not qualify as “post-filter[ed] residue.” *Id.*

IPR2023-00888

Patent 7,159,237 B2

Patent Owner further contends that the '237 patent supports its interpretation of the claim because “the anomaly engine, which performs the further analysis, is distinct from the positive and negative filtering subsystems that produce the “post-filtering residue.” Sur-Reply 1–2 (citing Ex. 1001, 8:50–57).

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time for the reasons discussed below.

Claim 1 specifies that the analysis of status data must include “filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.” The specification explains that, in one embodiment, “data is first filtered by negative filtering subsystem 2020, which discards uninteresting information, and then by positive filtering subsystem 2030, which selects possibly interesting information and forwards it to communications and resource coordinator 2060.” Ex. 1001, 8:45–50. According to the '237 patent, “[d]ata neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030 form the ‘residue,’ which is sent to anomaly engine 2050 for further analysis.” *Id.* at 8:5–53. Figure 2 of the '237 shows anomaly engine 2050 as a separate box or entity from negative filtering subsystem 2020, which in turn is shown as a separate box or entity from positive filtering subsystem 2030. *Id.* at Fig. 2.

Based on the current record, we agree with Petitioner that the IP addresses in undergo both positive (ALLOW filters) and negative (BLOCK filters) filtering and the remaining IP address information is not discarded but it targeted for deferred action filters, which appears to quality as

IPR2023-00888

Patent 7,159,237 B2

“analysis” per the ’237 patent. *See* Ex. 1001, 8:45–57; Ex. 1004, 4:27–30, 4:46–5:29.

Contrary to Patent Owner’s argument that “the filtering process must be distinct from the analysis that follows the filtering,” there is nothing in the claims or the specification that commands such distinction. Rather, the claims merely require that filtering is followed by an analysis of post-filtering residue. And, if we accept the district court’s claim construction of “post-filtering residue,” then any status data that has been neither discarded by negative filtering nor selected by positive filtering would qualify. *See* Ex. 1013, 4.

Patent Owner’s arguments do not appear to be commensurate with the scope of the claims, but appear to be an attempt to import limitations from specific embodiments into the claims. *See* Prelim. Resp. 37–38; *see* Ex. 1001, 8:5–53, Fig. 2. In keeping with the guidance from our reviewing court, we decline to read limitations from embodiments into the claims. *See Ericsson, Inc. v. D-Link Systems, Inc.*, 773 F.3d 1201, 1218 (Fed. Cir. 2014) (stating that although patent claims must be read in light of the specification, it is important that a court avoids importing limitations from the specification into the claims); *3M Innovative Properties Co. v. Tredegar Corp.*, 725 F.3d 1315, 1321 (Fed. Cir. 2014) (“While we construe the patent’s claims in light of the specification, limitations discussed in the specification may not be read into the claims.”); *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (holding that limitations are not to be read from the specification into the claims).

IPR2023-00888

Patent 7,159,237 B2

e) “*transmitting information about said identified events to an analyst associated with said security monitoring system*”

Petitioner contends that the combined teachings of Duvall and Chu combination teach this element because a person of ordinary skill in the art would have looked to Chu to optimize the handling of unresolved residue data in order to avoid “filtering too much or too little” in Duvall.” Pet 38 (citing Ex. 1004, 8:6–8; Ex. 1003 ¶ 136–137). Petition argues that “[i]n the case of unresolved data, Chu prompts for human intervention, which “would take the form of someone trained to manage Duvall’s corporate network.” *Id.* (citing Ex. 1003 ¶ 137). Petition further argues that Duvall’s use of “uniform set of filters” for a corporate network means that “the decision of how to handle unresolved data would not be left to each user individually, but rather, to a person trained in making such decisions, such as analysts at a network-security service.” *Id.* at 39 (citing Ex. 1004, 8:18–23; Ex. 1003 ¶¶ 138–139). Indeed, according to Petitioner, Duvall discloses a “password protected” “editing manager” indicating that the person editing filters in a corporate network is someone trained to manage the system. *Id.* at 39–40 (citing Ex. 1004, 8:8–10; Ex. 1003 ¶ 139). Thus, Petitioner concludes that “in the Duvall-Chu combination, information about the unresolved residue data would be sent to a trained network analyst for handling of the unresolved residue data.” *Id.* at 40–41.

Patent Owner disputes Petitioner’s position arguing that Duvall only teaches a first level of analysis by the filter system and the combination of Duvall and Chu fails to teach second level of analysis by an analyst. Prelim. Resp. 38–43 (citing Ex. 2001 ¶ 150). Patent Owner argues that neither Duval nor Chu provides a suggestion to transmit information about previously identified events from a first-level of analysis to an analyst who

IPR2023-00888

Patent 7,159,237 B2

can determine whether the potential events are actual events and/or resolve them. *Id.* at 39 (citing Ex. 2001 ¶ 153), 42. According to Patent Owner, Chu does not fill the gaps in Duvall regarding transmitting to an analyst because (1) Chu does not have a first level of analysis that would trigger transmission to an analyst and (2) Chu does not “transmit” information to an analyst. *Id.* at 39–40, 42.

Patent Owner contends that Chu only filters URLs with whitelists and blacklists to automate a trust decision process but “[i]f the trust decision cannot be automated because the URL is neither in the whitelist nor the blacklist, then Chu simply returns control back to the end-user—alerting them that no decision could be made.” Prelim. Resp. 40 (citing Ex. 1005, 44). Patent Owner argues that this is Chu’s “user intervention,” which does not qualify as “transmitting information about said identified events to an analyst.” *Id.* (citing Ex. 2001 ¶ 156; EX1001, 2:36–43). Patent Owner further argues that it would not be logical “to redirect the alert away from the end-user to a (non-existent) analyst for any reason” and that there is not explanation of how to introduce an analyst into either Duvall or Chu. *Id.* (citing Ex. 2001 ¶ 157), 43.

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time for the reasons discussed below. Given the specific information disclosed in the both Duvall and Chu, we agree with Petitioner that the prior art contemplates transmitting information to a skilled user or analyst for further action. *See* Ex. 1004, 8:6–10, 8:18–23; Ex. 1005, 44). Additionally, we are not persuaded at this time by Patent Owner’s argument, which appears to be

IPR2023-00888

Patent 7,159,237 B2

premised on attacking the references individually when the challenge is predicated on the combination of the prior art teachings.

f) “*receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system*”

Petitioner contends that the combined teachings of Duvall and Chu combination teach this element because each reference “discloses feedback in the form of an ‘editing Manager’ that allows ‘edit[ing] the database to add, delete, or modify filters in the database.” Pet. 41 (citing Ex. 1004, 8:2–5). According to Petitioner, a person of ordinary skill in the art at the critical time would have recognized that this feedback would be “*based on empirically-derived information reflecting operation of said security monitoring system*” because the information is only provided to the network analyst if the data is unresolved residue data—meaning that the data did not match any allow/block filters and passed through subsequent residue analysis (e.g., keywords and pattern matching) without any resolution. *Id.* (citing Ex. 1004, 5:8–19; Ex. 1003 ¶ 146). Therefore, Petitioner argues that decisions made by the trained network analyst (e.g., whether the filters should be modified) would be based on observable information about the data (e.g., transmission path, URL, etc.), and that feedback is received “*at the probe*” because Duvall’s editing manager is part of the filtering system implemented on server 30. *Id.* at 41–42 (citing Ex. 1004, 8:2–5 (“the filtering system has an editing Manager”), 8:18–21; Ex. 1003 ¶¶ 147–148).

Patent Owner has not provided any arguments regarding this specific claim limitation and the application of Duvall and Chu. Prelim. Resp. 31. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

IPR2023-00888

Patent 7,159,237 B2

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time. Specifically, we are satisfied because Duvall discloses the use of a password protected “editing Manager” that allows a user to edit “the database to add, delete, or modify filters in the database.” And, based on the current record, we agree with Petitioner’s position that a person of ordinary skill in the art at the critical time would have recognized that this feedback would meet the claims limitation because the information would be provided to the network analyst only upon detecting unresolved residue data. *See* Ex. 1004, 5:8–19.

g) “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback”

Petitioner contends the Duvall-Chu combination meets this limitation because Duvall “provid[es] updates online” so that “the system can adapt as new sites and servers are added to the Internet,” and Duvall’s filtering system accommodates dynamic updates because it searches “filter entries stored in the database” when performing its analysis so as to reflect changes to filters as they are edited. Pet. 43 (citing Ex. 1004, 2:16–18, 4:22–43, 8:3–16; Ex. 1003 ¶¶ 150–151); Reply 4 (“‘dynamically’ merely means ‘during actual operation, rather than offline’.”). Petitioner argues that editing the filters in Duvall’s filter database “modif[ies] an analysis capability of said probe . . . based on said feedback” because Duvall operates by comparing “information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken.” Pet. 42 (citing Ex. 1004, 4:22–27, 4:27–30, 4:40–43).

According to Petitioner, Duvall recognizes that “[b]ecause Internet sites are being added to the Internet at a fast rate . . . the filtering system

IPR2023-00888

Patent 7,159,237 B2

preferably also has an updating mechanism to keep filters current” and that “the system can adapt as new sites and servers are added to the Internet.” *Id.* (citing Ex. 1004, 7:18–21, 2:16–18). Petitioner further contends that “[g]iven the rapidity of updates, a POSA would have recognized that Duvall” needs to have dynamic modification of its probe’s “analysis capability. . . . during operation” because “taking the system offline each time an update was required would be disadvantageous.” *Id.* at 42–43 (citing Ex. 1003 ¶ 150). Petitioner concludes that “[t]o avoid this disadvantage, Duvall ‘provid[es] updates online’ so that ‘the system can adapt as new sites and servers are added to the Internet.’” *Id.* at 43 (citing Ex. 1004, 2:16–18); Pet. 42–43; Ex. 1003 ¶¶ 149–51.”).

We agree with Petitioner that the term “dynamically” means “during actual operation, rather than offline.” *See* Ex. 1001, 5:26–29 (the software and filters of the probe/sentry system 2000 . . . may be manually updated offline or dynamically (that is, during actual operation).” We do not agree, however, that simply because “dynamic modification” may offer advantages that it was, therefore, obvious. *See* Pet. 42–43; Reply 5.

The ’237 patent specifically teaches that updates that occur “dynamically” are updates made during actual operation. Ex. 1001, 5:26–29. As Patent Owner shows, “[t]he probe monitors and collects information from any component providing status data” “derived from traffic.” Prelim. Resp. 7 (citing Ex. 1001, 4:52–64). Although claim 1 indicates that “operation” “comprises” listed steps involving collecting, analyzing, and transmitting status data, claim 1 also indicates that “operation” includes receiving feedback, and dynamically modifying an analysis capability during operation thereof after receiving said feedback (i.e., “based on said feedback”). Because claim 1 is open-ended (i.e., recites “comprising” listing

IPR2023-00888

Patent 7,159,237 B2

the noted steps), this implies that the recited operation not only may involve one or more of the listed steps (after “receiving feedback at the probe”), but operation also may involve the probe monitoring devices for traffic, as indicated in Patent Owner’s description of the probe outlined above. *See id.* This understanding is further supported by the definition of “operation” found in the Microsoft Computer Dictionary 5th Ed. (*see* Ex. 3002 (“A specific action carried out by a computer in the process of executing a program.”)) and IEEE 100, The Authoritative Dictionary of IEEE Standard Terms, 7th Ed. (*see* Ex. 3003, “The process of running a computer system in its intended environment to perform its intended functions)), both of which reflect the common understanding of a person of ordinary skill in the art at the critical time.

Nevertheless, Petitioner fails to show sufficiently on this record how Duvall discloses dynamically modifying said probe during operation thereof after receiving feedback (“based on said feedback”). Petitioner points to Duvall’s editing manager and its disclosure of receiving automatic updates, but Petitioner does not explain sufficiently if editing or receiving updates occurs during some operation of the probe after receiving feedback, as called for in claim 1, as opposed to only manipulating the database. *See* Pet. 42–43. Petitioner also relies on Duvall’s teaching that it “operates by comparing ‘information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken,” but this fails to explain sufficiently how this comparison modifies an analysis capability of the probe during operation based on feedback. *See id.* at 42 (citing Ex. 1004, 4:22–

IPR2023-00888

Patent 7,159,237 B2

27).⁷ A comparison of the input data to the filter entries does not modify the analysis capability. Additionally, we do not find dynamic modification of an analysis capability of a probe to be one of “a finite number of identified, predictable solutions [that] a person of ordinary skill has good reason to pursue.” *See KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007). To be clear, this is not a matter of providing a person of ordinary skill with a simple design choice between two options. *See ACCO Brands Corp. v. Fellowes, Inc.*, 813 F.3d 1361, 1367 (Fed. Cir. 2016) (explaining that where an “ordinary artisan would . . . be left with two design choices . . . [e]ach of these two design choices is an obvious combination”). Rather, the

⁷ In other words, claim 1 is a method claim, not an apparatus claim that recites the mere capability of performing dynamic modification. *Cf. ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1361 (Fed. Cir. 2018) (“[A] prior art reference may anticipate or render obvious an apparatus claim—depending on the claim language—if the reference discloses an apparatus that is reasonably capable of operating so as to meet the claim limitations, even if it does not meet the claim limitations in all modes of operation.”); IPR2023-00888, Paper 9 (related institution decision involving an apparatus claim that recites the capability of the same dynamic modification). Petitioner fails to point to a disclosure in Duvall showing that its identified probe performs the step of “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.” Similarly, although claim 18 is an apparatus claim, it recites “said probe is *configured to* . . . dynamically modify an analysis capability of said probe during operation thereof based on said received feedback.” *See ParkerVision*, 903 F.3d at 1362 (noting that previous Federal Circuit “cases distinguish between claims with language that *recites capability*, and those that *recite configuration*,” and “where claim language recites ‘capability, as opposed to actual operation,’ *an apparatus that is ‘reasonably capable’ of performing the claimed functions ‘without significant alterations’ can infringe those claims.*” (quoting *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1217 (Fed. Cir. 2014) (emphasis added)). Similar remarks apply to claim 26, which recites “[a] computer-readable medium.”

IPR2023-00888

Patent 7,159,237 B2

recited claim limitation is a technical feature that is not taught or even suggested by the combined teachings of Duvall and Chu. Petitioner explains sufficiently that dynamic modification provides an advantage and why a skilled artisan would want to use it in solving a problem, but fails to sufficiently demonstrate that the prior art provided such a solution.

Petitioner's declarant, Dr. Jeffay, cites to the Zeise reference to support Petitioner's argument that a person of ordinary skill in the art would have "recognized that Duvall's 'analysis capability of said probe' is 'dynamically modified . . . during operation thereof' because taking the system offline each time an update was required would be disadvantageous." Ex. 1003 ¶ 150 (citing Ex. 1015, 1:54–2:6). Zeise discloses "dynamically distributing updates in a network." Ex. 1015, 1:7–9, 2:1–6. Zeise teaches (1) downloading and distributing updates in response to an automated or timed event (*id.* at 2:39–41) and (2) that sensors may automatically connect to a remote site and download new signatures (*id.* at 2:49–51). But neither Dr. Jeffay nor Petitioner sufficiently explain how Zeise's "dynamically distributing" compares to the '237 patent's "dynamic modification" or if Zeise's system makes modifications during operation.⁸ Nor does Dr. Jeffay sufficiently explain how Zeise dynamically modifies a sensor/probe or a system in response to feedback, such that it would have rendered such an act obvious to one of ordinary skill in the art. Rather, Zeise appears to be related to automated or timed update events. *See* Ex. 1015, 2:39–41.

⁸ Petitioner discusses Ziese in its third challenge in the Petition, specifically addressing dependent claims 14, 15, 25, 39, and 40. *See* Pet. 69–71. The Petition does not sufficiently answer the questions relating Ziese to "dynamic modification" at any point. In fact, Petitioner's explanation regarding Ziese's automation appears to cut against Dr. Jeffay's reliance on "dynamically distributing" for claim 1.

IPR2023-00888

Patent 7,159,237 B2

Accordingly, we find Petitioner fails to show that the combined teachings of Duvall and Chu would have rendered it obvious to “dynamically modif[y] an analysis capability of [a] probe during operation based on said received feedback” as required by independent claim 1.

h) Rationale to Combine the Teachings of Duvall and Chu

Petitioner contends a person of ordinary skill in the art would have had reason to combine the teaching of Duvall and Chu. Pet. 14–24 (citing Ex. 1003 ¶¶ 66–77, 94–111). Petitioner specifically argues that Duvall can implement default actions for filtering data that can lead to a “filtering system [] filtering too much or too little.” *Id.* at 20 (citing Ex. 1004, 8:6–8). Petitioner notes that “Duvall itself provides an ‘editing Manager’ that ‘allows the user to make custom changes if the user believes that the filtering system is filtering too much or too little.’” *Id.* (citing Ex. 1004, 8:2–8). Thus, according to Petitioner, a person of ordinary skill in the art “implementing Duvall’s system would have been motivated to seek techniques for more accurately resolving the status of residue data transmissions to ensure transmissions are correctly blocked or allowed.” *Id.* (citing Ex. 1003 ¶ 103). Petitioner argues that this would have led the skilled artisan to look for and locate Chu. *Id.* (citing Ex. 1003 ¶ 104).

Petitioner further contends that Chu is the same field of endeavor as Duvall and provides techniques for determining whether to block or allow residue data. *Id.* (citing Ex. 1005, 9, 44; Ex. 1003 ¶¶ 78–81, 92, 104). Petitioner argues that a person of ordinary skill in the art would have been motivated to incorporate Chu’s user intervention into Duvall’s system for data transmissions not matching any of Duvall’s positive/negative filters at step 104 of Figure 4, nor resolved by Duvall’s post-filtering residue analysis, and would have had a reasonable expectation of success for incorporating

IPR2023-00888

Patent 7,159,237 B2

such techniques. *Id.* at 22–23 (citing Ex. 1003 ¶¶ 107, 110; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 419–421 (2007)).

Patent Owner disputes Petitioner's position, arguing that Duvall and Chu have completely different focuses, and filter different things for different purposes in different ways. Prelim. Resp. 47–49. Patent Owner lists the following flaws it purports exists in the proposed combination of Duvall and Chu: (1) Duvall is unsuitable for use as a network security monitoring system; (2) Petitioner's Motivation Relies on a Mischaracterization of Duvall's concerns about subjectively "filtering too much or too little"; (3) Duvall and Chu use filters in different ways and for different purposes; (4) a person of ordinary skill in the art would not have combined Chu with Duvall given the differences in concerns, underlying assumptions, and goals; (5) Chu does not teach techniques for resolving the status of residue data; and (6) a person of ordinary skill in the art would not have arrived at the claims given the teachings of Duvall and Chu because (i) user intervention is not explained in Chu, and (ii) the combination would be inoperable. *Id.* at 49–64 (citing Ex. 2001 ¶¶ 179–219). Therefore, Patent Owner concludes that Petitioner has not shown that an ordinarily skilled artisan could have or would have made a combination with Duvall and Chu and arrived at the claimed invention. *Id.* at 47–48 (citing *Personal Web Tech. v. Apple Inc.*, 848 F.3d 987, 993–94 (Fed. Cir. 2017) (citing *Belden v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015))).

We agree with Patent Owner that Petitioner must articulate a reason why a person of ordinary skill in the art would have combined or modified the prior art references. *In re NuVasive, Inc.*, 842 F.3d 1376, 1382 (Fed. Cir. 2016); *see also Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1366 (Fed. Cir. 2017) ("In determining whether there would have

IPR2023-00888

Patent 7,159,237 B2

been a motivation to combine prior art references to arrive at the claimed invention, it is insufficient to simply conclude the combination would have been obvious without identifying any reason why a person of skill in the art would have made the combination.”); *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only could have made but would have been motivated to make the combinations or modifications of prior art to arrive at the claimed invention.”) (citing *InTouch Techs., Inc. v. VGO Commc’ns, Inc.*, 751 F.3d 1327, 1352 (Fed. Cir. 2014)).

After considering the arguments and evidence presented by the parties, we are persuaded Petitioner has adequately demonstrated that the person of ordinary skill in the art would have had reason to combine Duvall and Chu. The references are in the same field of endeavor and both relate filtering and decisions related to filtered data from the internet in order to remove data from untrusted sites. *See* Ex. 1004, 1:11–24, 2:12–18; Ex. 1005, 3, 9–11, 44. We do not agree with Patent Owner that incorporating teachings from Chu into Duvall would render Duvall inoperable, not do we agree that Chu provides insufficient information regarding “user intervention” when Chu’s policy specifically states “[p]rompt me for my attention otherwise.” Accordingly, we are persuaded by Petitioner’s position that a person of ordinary skill in the art at the critical time would have understood the implications and results of “user intervention” as taught by Chu and how it would have been (and not just could have been) incorporated into Duvall given Duvall’s teachings for a password protected “editing Manager.” *See* Ex. 1004, 8:2–8.

IPR2023-00888

Patent 7,159,237 B2

2. *Analysis of Claims 2–7, 15–23, 26–32, and 40–42*

Independent claims 18 and 26 each recite “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback,” which is recited in independent claim 1. *See* Ex. 1001, 35:55–57, 36:61–63, 37:41–43. All dependent claims depend directly or indirectly from independent claims 1, 18, or 26, and therefore, require the same ability for “dynamically modifying.” *See id.* at 35:58–36:37, 36:64–37:23, 37:44–38:47.

Having reviewed Petitioner’s arguments and supporting evidence in this present record, including the arguments summarized above for claim 1, we determine Petitioner has not established adequately for purposes of this Decision that the combination of Duvall and Chu discloses the limitations of claims 2–7, 15–23, 26–32, and 40–42 for the same reasons Petitioner did not meet its burden regarding claim 1. Accordingly, we determine Petitioner has not demonstrated a reasonable likelihood that these claims would have been rendered obvious to a person of ordinary skill in the art at the critical time by the combined teachings of Duvall and Chu.

B. Alleged Obviousness of Claims 7–13, 16, 24, 32–38, and 41 in view of Duvall, Chu, and Trcka

Petitioner contends dependent claims 7–13, 16, 24, 32–38, and 41 would have been obvious to person of ordinary skill in the art in view of the combined teachings of Duvall, Chu, and Trcka. Pet. 50–69 (citing Ex. 1003 ¶¶ 198–219). Petitioner relies on Trcka’s “Audit” and “Problem Determination” applications to correlate “*status data*” and other data from different devices to “particular types of network problems” occurring within a specific timeframe. *Id.* at 62 (citing Ex. 1014 ¶¶ 112, 116; Ex. 1003 ¶ 204).

IPR2023-00888

Patent 7,159,237 B2

Patent Owner does not specifically dispute Petitioner's contentions regarding this challenge. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Petitioner citations to and reliance on Trcka do not remedy the deficiencies of Duvall and Chu, and therefore, the combined teachings do not teach or suggest “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback” as required by all the independent claims. *See* Ex. 1001, 35:55–57, 36:61–63, 37:41–43.

Accordingly, for the reasons discussed previously, we are not persuaded that Petitioner has established a reasonable likelihood of success on this challenge.

C. Alleged Obviousness of Claims 14, 15, 25, 39, and 40 in view of Duvall, Chu, Trcka, and Ziese

Petitioner contends dependent claims 14, 15, 25, 39, and 40 would have been obvious to person of ordinary skill in the art in view of the combined teachings of Duvall, Chu, Trcka, and Ziese. Pet. 69–76 (citing Ex. 1003 ¶¶ 87–91, 221–232). Petitioner relies on Ziese to show correlation of data across multiple different probes (*id.* at 74–75) and for self-tuning probes (*id.* at 75–76) because Ziese discloses techniques in which “programs are automatically updated by downloading and distributing an update in response to an automated event.” *Id.* at 75 (citing Ex. 1015, 2:39–41). According to Petitioner, “the automated process ensures that updates are distributed when they are available, rather than waiting for a user to initiate the update process.” *Id.* at 75 (citing Ex. 1015, 1:54–67; Ex. 1003, ¶231).

Patent Owner does not specifically dispute Petitioner's contentions regarding this challenge. *See generally* Prelim. Resp. Nonetheless, the

IPR2023-00888

Patent 7,159,237 B2

burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Petitioner citations to and reliance on Ziese do not remedy the deficiencies of Duvall and Chu, and therefore, the combined teachings do not teach or suggest “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback” as required by all the independent claims. *See* Ex. 1001, 35:55–57, 36:61–63, 37:41–43.

Accordingly, for the reasons discussed previously, we are not persuaded that Petitioner has established a reasonable likelihood of success on this challenge.

V. CONCLUSION

After consideration of the Petition, the Preliminary Response, and the evidence of record, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that any of claims 1–42 of the ’237 Patent is unpatentable on any asserted ground. On this record, we decline to institute *inter partes* review of 1–42 of the ’237 Patent.

VI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that an *inter partes* is not instituted.

IPR2023-00888

Patent 7,159,237 B2

PETITIONER:

Jonathan Tuminaro

Dan Block

Michael Specht

Steven Pappas

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

jtuminar-ptab@sternekessler.com

dblock-ptab@sternekessler.com

mspecht-ptab@sternekessler.com

spappas-ptab@sternekessler.com

PATENT OWNER:

Nolan M. Goldberg

Baldassare Vinti

PROSKAUER ROSE LLP

NGoldbergPTABMatters@proskauer.com

BVinti@proskauer.com

Jonathan A. Roberts

NIXON & VANDERHYE P.C.

jr@nixonvan.com

EXHIBIT 3

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

BRITISH TELECOMMUNICATIONS PLC)	
and BT AMERICAS, INC.,)	
)	
Plaintiffs,)	
)	C. A. No. 22-1538-CJB
V.)	
)	JURY TRIAL DEMANDED
PALO ALTO NETWORKS, INC.,)	
)	
Defendant.)	

**PLAINTIFFS' OBJECTIONS AND RESPONSES TO DEFENDANT
PALO ALTO NETWORK, INC.'S FIRST SET OF INTERROGATORIES (NOS. 1-11)**

Pursuant to Rules 26 and 33 of the Federal Rules of Civil Procedure and the Court's orders in this action, Plaintiffs British Telecommunications plc and BT Americas, Inc. (collectively "BT") hereby object and respond to Defendant Palo Alto Network, Inc.'s ("PAN") First Set of Interrogatories (Nos. 1–11) served on September 29, 2023.

PRELIMINARY STATEMENT AND GENERAL OBJECTIONS

1. The following responses are made solely for the purpose of, and in relation to, this litigation. The following responses are based on the facts and information presently known and available to BT. Discovery is ongoing in this litigation and further investigation may disclose the existence of additional facts, add meaning to known facts, establish entirely new factual conclusions or legal contentions, or possibly lead to additions, variations, and changes to these responses. BT reserves the right to change or supplement these responses as additional facts are discovered, revealed, recalled, or otherwise ascertained.

2. BT objects to any interrogatory to the extent that it seeks information and documents protected from discovery under: (a) the attorney-client privilege; (b) the attorney work-product

- Joseph Yang (outside prosecution counsel)
- Thomas Raleigh Lane (outside prosecution counsel)

The identity of people, other than the named inventors, involved in filing and/or prosecution of the '641 Application are:

- Ronald S. Laurie (outside prosecution counsel)
- Joseph Yang (outside prosecution counsel)
- Thomas Raleigh Lane (outside prosecution counsel)

INTERROGATORY NO. 3:

State whether You contend that any of Your products practice one or more claims of the Asserted Patents. For each product that You contend practices one or more claims of the Asserted Patents state all bases under which You contend each Asserted Claim is practiced or not practiced by each product (including a chart identifying specifically where each limitation of each Asserted Claim is found within each product or a statement that the limitation is not found in the product and whether each limitation of each Asserted Claim that You assert is present is alleged to be literally present in each product on the one hand or present under the doctrine of equivalents on the other hand), separately for each limitation of each Asserted Claim state all facts on which You rely for your assertions, and separately for each limitation of each Asserted Claim identify all Documents and circumstances relating to those facts and all persons with knowledge of those facts.

RESPONSE:

In addition to the Preliminary Statement and General Objections, BT objects to this interrogatory as overbroad and unduly burdensome because it requires BT to produce a claim chart for products that are not relevant to any claim or defense. As BT explains in response to Interrogatories No. 5 and 6, BT is not seeking lost profits for the accused products or an injunction.

OF COUNSEL:

Bart H. Williams
PROSKAUER ROSE LLP
2029 Century Park East
Suite 2400
Los Angeles, California 90067
310-557-2900
bwilliams@proskauer.com

Baldassare Vinti
Nolan M. Goldberg
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
212-969-3000
bvinti@proskauer.com
ngoldberg@proskauer.com

Edward Wang
PROSKAUER ROSE LLP
1001 Pennsylvania Avenue NW
Suite 600
Washington, DC 20004
202-416-6800
ewang@proskauer.com

Dated: October 30, 2023
11138409

POTTER ANDERSON & CORROON LLP

By: /s/ Philip A. Rovner
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

*Attorneys for Plaintiff British
Telecommunications plc and
BT Americas, Inc.*

CERTIFICATE OF SERVICE

I, Philip A. Rover, hereby certify that on October 30, 2023, I served the foregoing document by forwarding the document by electronic transmission to the email addresses listed below:

BY EMAIL

Brian E. Farnan
Michael J. Farnan
FARNAN LLP
919 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 777-0300
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Adrian C. Percer
Gregg T. Stephenson
WEIL, GOTSHAL & MANGES LLP
201 Redwood Shores Parkway
Redwood Shores, CA 94065
(650) 802-3000
Adrian.percer@weil.com
Gregg.stephenson@weil.com

Anish R. Desai
Tom Yu
WEIL, GOTSHAL & MANGES LLP
767 Fifth Avenue
New York, NY 10153
(212) 310-8000
anish.desai@weil.com
tom.yu@weil.com

Priyata Y. Patel
WEIL, GOTSHAL & MANGES LLP
2001 M Street, NW Suite #600
Washington, D.C. 20036
(202) 682-7000
priyata.patel@weil.com
Attorneys for Defendant

By: /s/ Philip A. Rovner
Philip A. Rovner (#3215)

EXHIBIT 4



End-of-Life Summary

- PAN-OS & Panorama
- Traps, ESM and Cortex XDR agent
- GlobalProtect™
- Prisma Cloud Compute Edition
- LightCyber Magna Virtual Appliances
- Evident.io™
- Prisma SD-WAN
- BRIGHTCLOUD Subscription
- VM-Series Models

PAN-OS & Panorama

Version	Release Date	End-of-Life Date
11.1	November 3, 2023	May 3, 2026
11.0	November 17, 2022	November 17, 2024
10.2 ^{^^^}	February 27, 2022	August 27, 2025
10.1 [‡]	May 31, 2021	December 1, 2024
10.0 ^{^^}	July 16, 2020	July 16, 2022
9.1 ⁺⁺	December 13, 2019	March 31, 2024

9.0-XFR (VM-Series only)	September 19, 2019	September 19, 2020
9.0	February 6, 2019	March 1, 2022
8.1 ⁺	March 1, 2018	March 1, 2022
8.0	January 29, 2017	October 31, 2019
7.1	March 29, 2016	June 30, 2020
7.0	June 4, 2015	December 4, 2017
6.1	October 25, 2014	October 25, 2018
6.0	January 19, 2014	March 19, 2017
5.1 (Panorama only)	May 9, 2013	May 9, 2017
5.0	November 13, 2012	November 13, 2016
4.1	October 31, 2011	April 30, 2015
4.0	February 22, 2011	December 31, 2014
3.1	March 15, 2010	June 30, 2013
3.0	June 17, 2009	December 17, 2010
2.1	January 5, 2009	January 5, 2012
2.0	May 20, 2008	May 20, 2009
1.3	November 15, 2007	November 20, 2008

⁺ PAN-OS 8.1 will be supported past the End-of-Life date only for specific hardware model(s) with the Last Supported OS of PAN-OS 8.1 and only until the respective End-of-Life date of the hardware listed on the [hardware end-of-life summary page](#) .

⁺⁺ PAN-OS 9.1 will be supported past the End-of-Life date only for specific hardware model(s) with the Last Supported OS of PAN-OS 9.1 and only until the respective End-of-Life date of the hardware

listed on the [hardware end-of-life summary page](#).

^^^ PAN-OS 10.0 will be supported past the End-of-Life date only for specific hardware model(s) with the Last Supported OS of PAN-OS 10.0 and only until the respective End-of-Life date of the hardware listed on the [hardware end-of-life summary page](#) .

‡ PAN-OS 10.1 will be supported past the End-of-Life date only for specific hardware model(s) with the Last Supported OS of PAN-OS 10.1 and only until the respective End-of-Life date of the hardware listed on the [hardware end-of-life summary page](#) .

^^^^ PAN-OS 10.2 will be supported past the End-of-Life date only for specific hardware model(s) with the Last Supported OS of PAN-OS 10.2 and only until the respective End-of-Life date of the hardware listed on the [hardware end-of-life summary page](#) .

Traps, ESM and Cortex XDR agent

Version	Release Date	End-of-Life Date
8.1 (Cortex XDR agent)	June 25, 2023	April 9, 2024
8.0 (Cortex XDR agent)	March 5, 2023	December 19, 2023
7.9 CE (Cortex XDR agent)	March 19, 2023	March 19, 2025
7.9 (Cortex XDR agent)	December 4, 2022	September 11, 2023
7.8 (Cortex XDR agent)	July 24, 2022	April 24, 2023
7.7 (Cortex XDR agent)	March 27, 2022	December 27, 2022
7.6 (Cortex XDR agent)	December 5, 2021	September 5, 2022
7.5 CE (Cortex XDR Agent)	March 6, 2022	March 6, 2024
7.5 (Cortex XDR agent)	August 22, 2021	August 22, 2022
7.4 (Cortex XDR agent)	May 24, 2021	May 24, 2022
7.3 (Cortex XDR agent)	February 1, 2021	February 1, 2022

7.2 (Cortex XDR agent)	September 07, 2020	March 07, 2022
7.1 (Cortex XDR agent)	April 22, 2020	June 4, 2021
7.0 (Cortex XDR agent)	December 4, 2019	June 4, 2021
6.1	July 2, 2019	July 1, 2022
6.0	February 26, 2019	February 26, 2020
5.0	March 19, 2018	June 1, 2024
4.2	June 25, 2018	March 1, 2022*
4.1	September 15th, 2017	September 15, 2019
4.0	April 5th, 2017	April 5, 2018
3.4	August 21, 2016	August 21, 2019
3.3	November 10th, 2015	February 28, 2017
3.2	March 31st, 2015	March 31, 2016
3.1	September 3rd, 2014	September 3, 2015

**4.2 will be the last ESM-based feature release.*

GlobalProtect™

GlobalProtect App version	Release Date	End-of-Engineering Date	End-of-Life Date
6.2	05/23/2023	05/23/2025	05/23/2025
6.1	09/01/2022	09/01/2024	09/01/2024
6.0	02/22/2022	02/22/2025	02/22/2025
5.3	06/01/2021	12/01/2022	06/01/2023

5.2	07/30/2020	08/31/2023	02/28/2024
5.1	12/12/2019	03/12/2021	12/31/2024
5.0	2/12/2019	5/12/2020	2/12/2021
4.1	3/1/2018	6/1/2019	3/1/2020
4.0	1/30/2017	5/2/2018	1/30/2019
3.1	6/23/2016	9/23/2017	6/23/2018
3.0	2/16/2016	5/18/2017	2/15/2018

**GlobalProtect App 5.1 End-of-Life has been extended to provide continued FIPS-CC support. Please note that the End-of-Engineering date has not been extended.*

For more details, see [Palo Alto Networks End-of-Life Policy](#).

Prisma Cloud Compute Edition

Version	Release Date	End-of-Life Date
22.06	June 9, 2022	August 20, 2023
22.01	January 10, 2022	April 23, 2023
21.08	September 08, 2021	December 04, 2022
21.04	April 26, 2021	June 9, 2022
20.12	December 21, 2020	September 8, 2021
20.09	September 22, 2020	April 26, 2021
20.04	April 07, 2020	December 21, 2020
19.11	November 20, 2019	September 22, 2020

For more details, see [Support Lifecycle](#).

LightCyber Magna Virtual Appliances

End-of-Sale Product	End-of-Sale Date	End-of-Life Date	Resources	Last Supported OS
LightCyber Magna Detector Virtual Appliance (D-150V)	December 31, 2017	December 31, 2020	LightCyber Behavioral Analytics Datasheet	Magna 3.9
LightCyber Magna Probe Virtual Appliance (P-50TV)	December 31, 2017	December 31, 2020	LightCyber Behavioral Analytics Datasheet	Magna 3.9
LightCyber Magna Master Virtual Appliance (M-100V)	December 31, 2017	December 31, 2020	LightCyber Behavioral Analytics Datasheet	Magna 3.9

Evident.io™

Platform	Release Date	End-of-Support Date	End-of-Life Date	
Evident.io	03/26/2018	07/31/2020	12/31/2020	Announcement

Prisma SD-WAN

Version	Release Date	End-of-Life Date
6.2	05/04/2023	05/04/2025
6.1	12/23/2022	12/23/2024
6.0	11/05/2022	09/01/2023
5.6	10/05/2021	11/05/2024
5.5	04/11/2021	08/30/2023
5.4	08/10/2020	03/31/2023
5.2	02/05/2020	01/31/2022
5.1	01/31/2019	01/31/2022
5.0	08/03/2018	01/31/2022
4.7	05/23/2018	03/15/2020
4.6	04/04/2018	02/15/2020
4.5	09/15/2017	02/15/2020
4.4	04/28/2017	02/15/2020

BRIGHTCLOUD Subscription

Product	Release Date	End-of-Life Date
BrightCloud	January 5, 2009	July 31, 2021

BrightCloud licenses can be migrated to PAN-DB at no additional cost


VM-Series Models

End-of-Sale Product	End-of-Sale Date	End-of-Life Date	Resources	Last Supported OS
VM-Series Models (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV)	July 31, 2021	July 31, 2024	Use Software NGFW Credits instead.	TBD

These fixed license VM-Series firewall models are being replaced by Software NGFW Credits, a new credit-based licensing model that supports flexible firewall sizes and flexible security subscriptions. Customers are advised to use **Software NGFW Credits** going forward as they offer much greater simplicity, flexibility, and agility.


Please note that this announcement does not apply to VM-Series firewall Pay-as-you-Go (PAYG) licenses sold in the Public Cloud Marketplaces (AWS, Azure, GCP, Oracle) and via the Cloud Security Service Provider (CSSP) program.

Recommended Resources



Webinar

Evolving AppSec for



Discover why we need to rethink our approach to cloud-



Video

Simplifying Security Through

All around us, digital transformation continues to

June 30, 2023

February 9, 2023



Datasheet
PA-400 Series
 Palo Alto Networks
 PA-400 series ML-
 Powered NGFW (PA-
 November 8, 2023



Infographic
**5 Effective Steps to
 Protect Against**
 What steps should
 organizations take to
 improve cyber
 December 2, 2022



Article
**What is a denial
 of service attack**
 A Denial-of-Service
 (DoS) attack is an
 attack meant to shut
 December 13, 2022



Resource
PA-1400 Series
 Palo Alto Networks
 PA-1400 series ML-
 Powered NGFW (PA-
 July 19, 2023

Get the latest news, invites to events, and threat alerts

Your email

Sign Up →

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).

Popular Resources

[Blog](#)

[Communities](#)

[Content Library](#)

[Cyberpedia](#)

[Event Center](#)

[Investors](#)

[Products A-Z](#)

Legal Notices

[Privacy](#)

[Trust Center](#)

[Terms of Use](#)

[Documents](#)

Popular Links

[About Us](#)

[Customers](#)

[Careers](#)

[Contact Us](#)

[Manage Email Preferences](#)

[Newsroom](#)

[Product Certifications](#)


[Report a Vulnerability](#)

[Tech Docs](#)

[Unit 42](#)

[Sitemap](#)



 EN 

[Create an account or login →](#)

Copyright © 2023 Palo Alto Networks. All rights reserved

EXHIBIT 5

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

BRITISH TELECOMMUNICATIONS PLC)	
and BT AMERICAS, INC.,)	
)	
Plaintiffs,)	
)	C. A. No. 22-1538-CJB
v.)	
)	JURY TRIAL DEMANDED
PALO ALTO NETWORKS, INC.,)	
)	
Defendant.)	

INITIAL INFRINGEMENT CONTENTIONS

Pursuant to Section 4.c of the Default Standard for Discovery, Paragraph 6(d) of the Scheduling Order (D.I. 62), Plaintiffs British Telecommunications plc and BT Americas, Inc. (collectively, “BT”) present their Initial Infringement Contentions as to Defendant Palo Alto Networks, Inc. (“PAN”). These Initial Infringement Contentions provide a claim chart relating PAN’s accused products or services (“Accused Products”) to the asserted claims of U.S. Patent Nos. 7,159,237 (the “’237 Patent”) and 7,895,641 (the “’641 Patent”) (collectively, the “Asserted Patents”) that are infringed by the Accused Products.

Based on the information currently available to BT, BT contends that the Accused Products made, used, sold, offered for sale, and/or imported into the United States, or provided in a manner creating liability for PAN under sections of 35 U.S.C. § 271 (including, *e.g.*, for inducement of infringement), from November 28, 2016 to the expiration of the asserted patents, infringe the claims of the Asserted Patents, as specified in the charts attached hereto as Exhibit A. While BT contends that PAN literally infringes each asserted claim, to the extent a claim limitation is not met literally, it is met under the Doctrine of Equivalents.

These Initial Infringement Contentions are based on PAN's production of core technical documents pursuant to Default Standard Paragraph 4.b and Paragraph 6(c) of the Scheduling Order (D.I. 62), and information reasonably available to BT, without the benefit of full fact discovery and without the benefit of the Court's claim constructions. To date, PAN has failed to produce a complete set of core technical documents for the Accused Products, which were identified in BT's Amended Identification of Accused Products Pursuant to Paragraph 4(a) of the Default Standard for Discovery on October 3, 2023 (D.I. 80). BT's Initial Infringement Contentions are not an admission, adoption, or waiver of any particular claim construction, which BT will propose according to the Scheduling Order (D.I. 62).

BT identifies the following asserted claims of the Asserted Patents and the infringing Accused Products for each Asserted Patent:

Asserted Patent	Asserted Claims	Accused Products¹
'237 Patent	1-2, 6, 8, 10, 12, 14-18, 24-26	<i>See</i> BT's Amended Identification of Accused Products Pursuant to Paragraph 4(a) of the Default Standard For Discovery, II.A.
'641 Patent	1-2, 6, 8, 10, 12, 14-22, 25	<i>See</i> BT's Amended Identification of Accused Products Pursuant to Paragraph 4(a) of the Default Standard For Discovery, II.B.

Certain information about PAN's Accused Products is not available without engaging in further discovery, including, for example, discovery of the operation of certain internal and proprietary systems and processes and, to the extent it may be required, relevant source code. Further, infringement investigations are ongoing, and BT anticipates that additional facts and relevant documents will be uncovered and disclosed that could create good cause for further

¹ Certain model numbers of Accused Products are identified by way of example and are not intended to be an exhaustive list of infringing products.

supplementation and/or amendment of these contentions. Accordingly, BT reserves the right to supplement or amend these initial claim charts and contentions in this case when discovery is complete and/or pursuant to the Federal Rules of Civil Procedure, the Default Standard, and Court Orders.

OF COUNSEL:

Bart H. Williams
PROSKAUER ROSE LLP
2029 Century Park East
Suite 2400
Los Angeles, California 90067
310-557-2900
bwilliams@proskauer.com

Baldassare Vinti
Nolan M. Goldberg
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
212-969-3000
bvinti@proskauer.com
ngoldberg@proskauer.com

Edward Wang
PROSKAUER ROSE LLP
1001 Pennsylvania Avenue NW
Suite 600
Washington, DC 20004
202-416-6800
ewang@proskauer.com

Dated: November 17, 2023

POTTER ANDERSON & CORROON LLP

By: /s/ Philip A. Rovner
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

*Attorneys for Plaintiff British
Telecommunications plc and
BT Americas, Inc.*

CERTIFICATE OF SERVICE

I, Philip A. Rover, hereby certify that on November 17, 2023, I served the foregoing document by forwarding the document by electronic transmission to the email addresses listed below:

BY EMAIL

Brian E. Farnan
Michael J. Farnan
FARNAN LLP
919 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 777-0300
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Adrian C. Percer
Gregg T. Stephenson
Weil, Gotshal & Manges LLP
201 Redwood Shores Parkway
Redwood Shores, CA 94065
(650) 802-3000
Adrian.percer@weil.com
Gregg.stephenson@weil.com

Anish R. Desai
Tom Yu
WEIL, GOTSHAL & MANGES LLP
767 Fifth Avenue
New York, NY 10153
(212) 310-8000
anish.desai@weil.com
tom.yu@weil.com

Priyata Y. Patel
WEIL, GOTSHAL & MANGES LLP
2001 M Street, NW Suite #600
Washington, D.C. 20036
(202) 682-7000
priyata.patel@weil.com

Attorneys for Defendant

By: /s/ Philip A. Rovner
Philip A. Rovner (#3215)

EXHIBIT 6

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

BRITISH TELECOMMUNICATIONS PLC)	
and BT AMERICAS, INC.,)	
)	
Plaintiffs,)	
)	C.A. No. 22-01538-CJB
v.)	
)	JURY TRIAL DEMANDED
PALO ALTO NETWORKS, INC.,)	
)	
Defendant.)	

**PLAINTIFFS’ AMENDED IDENTIFICATION OF ACCUSED PRODUCTS PURSUANT
TO PARAGRAPH 4(a) OF THE DEFAULT STANDARD FOR DISCOVERY**

Plaintiffs British Telecommunications plc and BT Americas, Inc. (collectively “Plaintiffs”) respectfully submit, pursuant to Paragraph 6(b) of the Scheduling Order jointly submitted by the parties (D.I. 62), in conjunction with Paragraph 4(a) of the Default Standard for Electronic Discovery (“Default Standard”), and subject to continuing investigation, the following amended disclosures:

I. REQUIRED PRODUCTION OF FILE HISTORIES

Pursuant to Paragraph 4(a) of the Default Standard, Plaintiffs provided certified copies of U.S. Patent Nos. 7,159,237 (the “’237 Patent”) and 7,895,641 (the “’641 Patent”) (collectively, the “Asserted Patents”) and the file history of each of the Asserted Patents with Plaintiffs’ Identification of Accused Products Pursuant to Paragraph 4(a) of the Default Standard for Discovery on September 21, 2023.

II. ACCUSED PATENTS AND THE PRODUCTS THEY INFRINGE

Pursuant to Paragraph 4(a) of the Default Standard, Plaintiffs provide the following amended preliminary identification of accused products made, used, sold, offered for sale, and/or imported into the United States by Defendant Palo Alto Networks, Inc. (“PAN”) (the “Accused

Products”), or in relation to which PAN is otherwise liable under 35 U.S.C. § 271 (e.g., as an indirect infringer), and the Asserted Patent(s) that they infringe. These disclosures are based on information reasonably available at this time. Plaintiffs have attempted to identify, using publicly available information without the benefit of any formal discovery, product names and/or model numbers of certain Accused Products. Further investigation and discovery may result in the need to amend or supplement this identification of Accused Products. Accordingly, the names and/or model numbers herein should not be read as an exhaustive listing of the names and model numbers of the Accused Products and should also be understood to include any products or services that operate in a substantially similar manner or are equivalents thereof from at least November 28, 2016 until the expiration of the Asserted Patents, respectively.

Plaintiffs reserve the right to modify, amend, supplement, or correct this identification of Accused Products, including as new products are discovered or released by PAN.

A. PAN Products That Infringe The ’237 Patent

Plaintiffs hereby disclose the following products or services made, used, sold, offered for sale, and/or imported into the United States, or provided in a manner creating liability under any section of 35 U.S.C. § 271, from at least November 28, 2016 to present, by PAN so as to infringe at least one claim of the ’237 Patent:

- PA-7000 Series
 - PA-7080
 - PA-7050
 - PAN-PA-7000-100G-NPC-A
 - PAN-PA-7000-DPC-A
- PA-5400 Series
 - PA-5410
 - PA-5420
 - PA-5430
 - PA-5440
 - PA-5450
 - PAN-PA-5400-DPC-A

- PA-5200 Series
 - PA-5280
 - PA-5260
 - PA-5250
 - PA-5220
- PA-3400 Series
 - PA-3410
 - PA-3420
 - PA-3430
 - PA-3440
- PA-3200 Series
 - PA-3260
 - PA-3250
 - PA-3220
- PA-1400 Series
 - PA-1420
 - PA-1410
- PA-800 Series
 - PA-850
 - PA-820
- PA-400 Series
 - PA-460
 - PA-450
 - PA-445
 - PA-440
 - PA-415
 - PA-410
- PA-220
- PA-220R
- CN-Series
- VM-Series
- PAN-OS
- Cloud NGFW
- Panorama

- WildFire® Service
- Prisma Access
- Prisma SASE
- PAN SD-WAN
- Unit42
 - Unit42 Managed Detection and Response
- Cortex

B. PAN Products That Infringe The '641 Patent

Plaintiffs hereby disclose the following products or services made, used, sold, offered for sale, and/or imported into the United States, or provided in a manner creating liability under any section of 35 U.S.C. § 271, from at least November 28, 2016 to present, by PAN so as to infringe at least one claim of the '641 Patent:

- PA-7000 Series
 - PA-7080
 - PA-7050
 - PAN-PA-7000-100G-NPC-A
 - PAN-PA-7000-DPC-A
- PA-5400 Series
 - PA-5410
 - PA-5420
 - PA-5430
 - PA-5440
 - PA-5450
 - PAN-PA-5400-DPC-A
- PA-5200 Series
 - PA-5280
 - PA-5260
 - PA-5250
 - PA-5220
- PA-3400 Series
 - PA-3410
 - PA-3420
 - PA-3430

- PA-3440
- PA-3200 Series
 - PA-3260
 - PA-3250
 - PA-3220
- PA-1400 Series
 - PA-1420
 - PA-1410
- PA-800 Series
 - PA-850
 - PA-820
- PA-400 Series
 - PA-460
 - PA-450
 - PA-445
 - PA-440
 - PA-415
 - PA-410
- PA-220
- PA-220R
- CN-Series
- VM-Series
- PAN-OS
- Cloud NGFW
- Panorama
- WildFire® Service
- Prisma Access
- Prisma SASE
- PAN SD-WAN
- Unit42
 - Unit42 Managed Detection and Response

- Cortex

C. Damages Model

BT is entitled to no less than an award of a reasonable royalty on PAN's infringing sales in accordance with 35 U.S.C. § 284, together with costs and interest and no less than a reasonable royalty and/or lost profits on convoyed sales. Further, as PAN's infringement has been willful, BT is entitled to trebling of the damage award and award of attorney's fees pursuant to 35 U.S.C. §§ 284, 285.

OF COUNSEL:

Bart H. Williams
PROSKAUER ROSE LLP
2029 Century Park East
Suite 2400
Los Angeles, California 90067
310-557-2900
bwilliams@proskauer.com

Baldassare Vinti
Nolan M. Goldberg
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
212-969-3000
bvinti@proskauer.com
ngoldberg@proskauer.com

Edward Wang
PROSKAUER ROSE LLP
1001 Pennsylvania Avenue NW
Suite 600
Washington, DC 20004
202-416-6800
ewang@proskauer.com

Dated: October 2, 2023

POTTER ANDERSON & CORROON LLP

By: /s/ Philip A. Rovner
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

*Attorneys for Plaintiff British
Telecommunications plc and
BT Americas, Inc.*

CERTIFICATE OF SERVICE

I, Philip A. Rover, hereby certify that on October 2, 2023, I served Plaintiffs' Initial Disclosures Pursuant to Fed. R. Civ. P. 26(a)(1) by forwarding the document by electronic transmission to the email addresses listed below:

BY EMAIL

Brian E. Farnan
Michael J. Farnan
FARNAN LLP
919 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 777-0300
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Adrian C. Percer
WEIL, GOTSHAL & MANGES LLP
201 Redwood Shores Parkway
Redwood Shores, CA 94065
(650) 802-3000
adrian.percer@weil.com

Anish R. Desai
Tom Yu
WEIL, GOTSHAL & MANGES LLP
767 Fifth Avenue
New York, NY 10153
(212) 310-8000
anish.desai@weil.com
tom.yu@weil.com

Priyata Y. Patel
WEIL, GOTSHAL & MANGES LLP
2001 M Street, NW Suite #600
Washington, D.C. 20036
Telephone: (202) 682-7000
priyata.patel@weil.com

Attorneys for Defendant

By: /s/ Philip A. Rovner
Philip A. Rovner (#3215)

EXHIBIT 7

Asserted Claims of U.S. 7,159,237	Instituted Claims of U.S. 7,895,641
1. A method of operating a probe as part of a security monitoring system for a computer network, comprising:	1. A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:
[1a] collecting status data from at least one monitored component of said network;	[1a] a sensor coupled to collect status data from at least one monitored component of the network;
[1b] analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;	[1b] a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
[1c] transmitting information about said identified events to an analyst associated with said security monitoring system;	[1c] a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
[1d] receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and	[1d] a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
[1e] dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.	[1e] a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.
2. The method of claim 1, wherein said identifying step includes performing a multi-stage analysis of said status data.	2. The system of claim 1, wherein the identifying step includes performing a multi-stage analysis of the status data.
6. The method of claim 2, wherein said multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from said probe.	6. The system of claim 2, wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe.

Asserted Claims of U.S. 7,159,237	Instituted Claims of U.S. 7,895,641
8. The method of claim 7, wherein said identifying step includes cross-correlating data across said monitored components.	8. The system of claim 7, wherein the identifying step includes cross-correlating data across the monitored components.
10. The method of claim 1, further comprising after said step (c), performing further computer-based analysis at a secure operations center configured to receive data from said probe.	10. The system of claim 1, further comprising after the step (c), a secure operations center coupled to perform further computer-based analysis and to receive data from the probe.
12. The method of claim 10, wherein said identifying step includes cross-correlating data across said monitored components.	12. The system of claim 10, wherein the identifying step includes cross-correlating data across the monitored components.
14. The method of claim 10, wherein said computer-based analysis includes cross-probe correlation.	14. The system of claim 10, wherein the computer-based analysis includes cross-probe correlation.
15. The method of claim 1, further comprising instantaneously self-tuning said probe based on previously collected status data.	15. The system of claim 1, further comprising instantaneously self-tuning the probe based on previously collected status data.
16. The method of claim 1, wherein said dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.	16. The system of claim 1, wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.
17. The method of claim 1, wherein said receiving feedback step occurs in substantially real time.	17. The system of claim 1, wherein the receiving feedback step occurs in substantially real time.
<p>18. A security monitoring system for a computer network, comprising:</p> <p>a) a plurality of sensors for monitoring components of said network;</p> <p>b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and</p> <p>c) at least one probe, wherein said probe is configured to</p>	<p>1. A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:</p>

Asserted Claims of U.S. 7,159,237	Instituted Claims of U.S. 7,895,641
[18(1)] collect status data from at least one sensor monitoring at least one component of said network;	[1a] a sensor coupled to collect status data from at least one monitored component of the network;
[18(2)] analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;	[1b] a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering
[18(3)] transmit information about said identified events to an analyst associated with said secure operations center;	[1c] a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
[18(4)] receive feedback based on empirically-derived information reflecting operation of said security monitoring system; and	[1d] a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
[18(5)] dynamically modify an analysis capability of said probe during operation thereof based on said received feedback	[1e] a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.
24. The security monitoring system of claim 18, wherein said secure operations center is configured to identify potentially security-related events by performing a computer-based analysis of said potentially security-related event data received from said probe.	10. The system of claim 1, further comprising after the step (c), a secure operations center coupled to perform further computer-based analysis and to receive data from the probe.
25. The security monitoring system of claim 24, wherein said computer-based analysis is configured to correlate data from different probes.	14. The system of claim 10, wherein the computer-based analysis includes cross-probe correlation.
26. A computer-readable medium whose contents cause a computer system to operate a probe as part of a security	1. A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:

Asserted Claims of U.S. 7,159,237	Instituted Claims of U.S. 7,895,641
monitoring system for a computer network, by performing the steps of:	
[26a] collecting status data from at least one monitored component of said network;	[1a] a sensor coupled to collect status data from at least one monitored component of the network;
[26b] analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;	[1b] a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
[26c] transmitting information about said identified events to an analyst associated with said security monitoring system;	[1c] a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
[26d] receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and	[1d] a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
[26e] dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.	[1e] a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

EXHIBIT 8

REDACTED

EXHIBIT 9



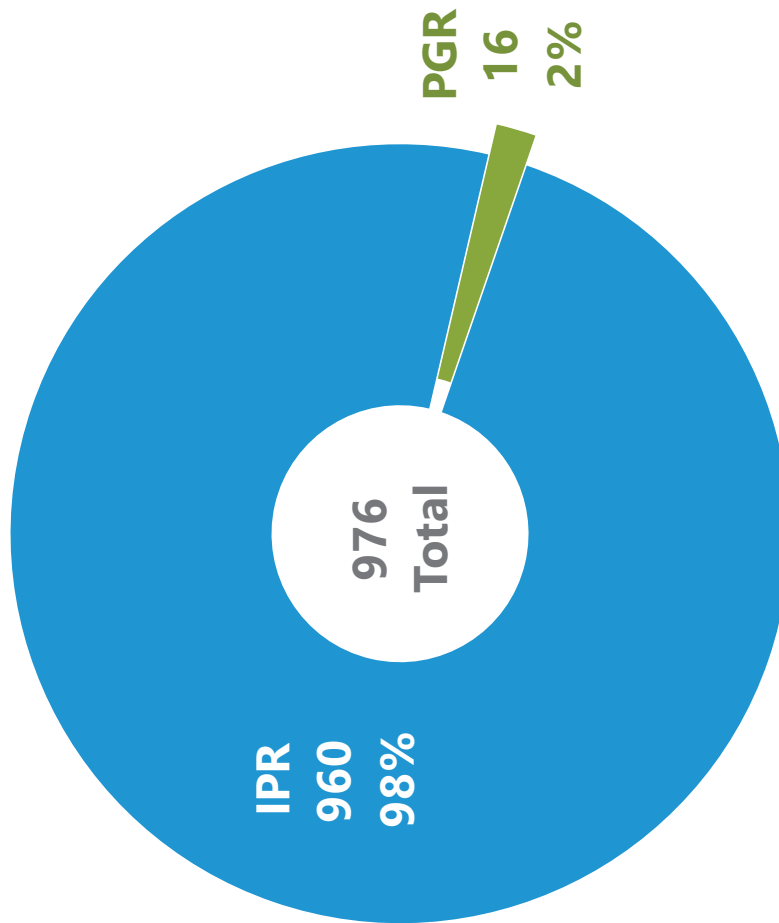
PTAB Trial Statistics FY23 Q3 Outcome Roundup IPR, PGR

**Patent Trial and Appeal Board
Fiscal Year 2023 3rd Quarter**

UNITED STATES
PATENT AND TRADEMARK OFFICE

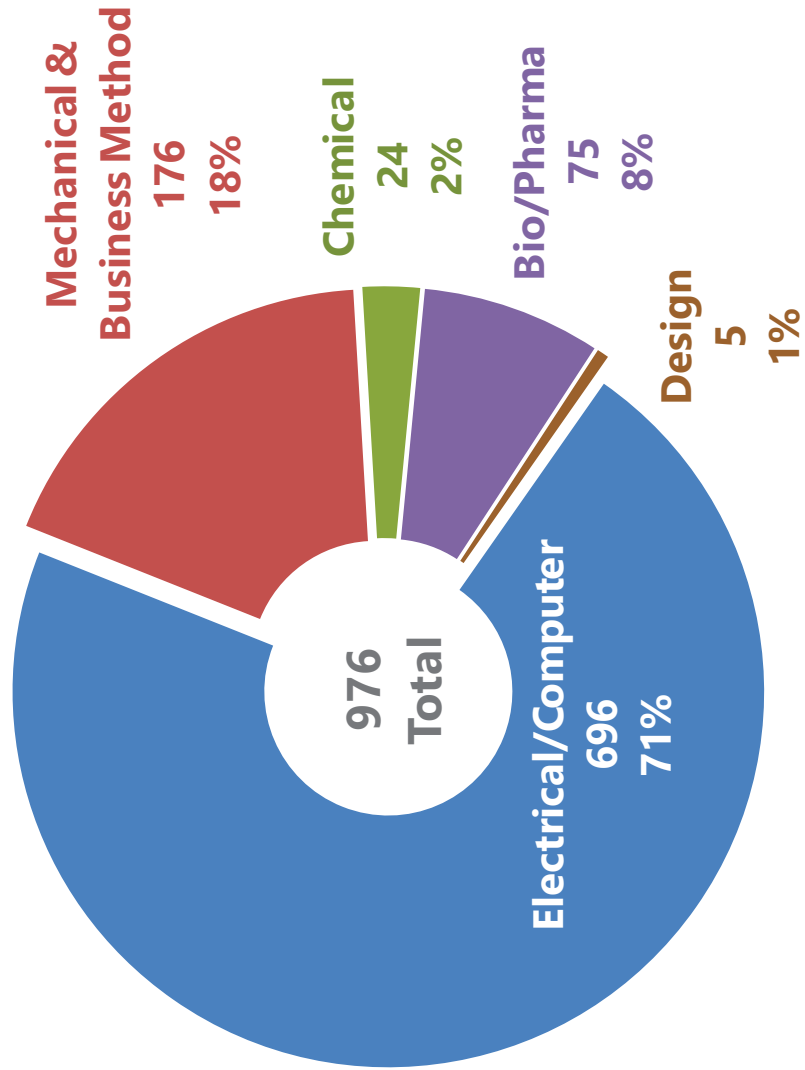
uspto

Petitions filed by trial type (FY23 through Q3: Oct. 1, 2022 to Jun. 30, 2023)



Trial types include Inter Partes Review (IPR) and Post Grant Review (PGR).

Petitions filed by technology (FY23 through Q3: Oct. 1, 2022 to Jun. 30, 2023)



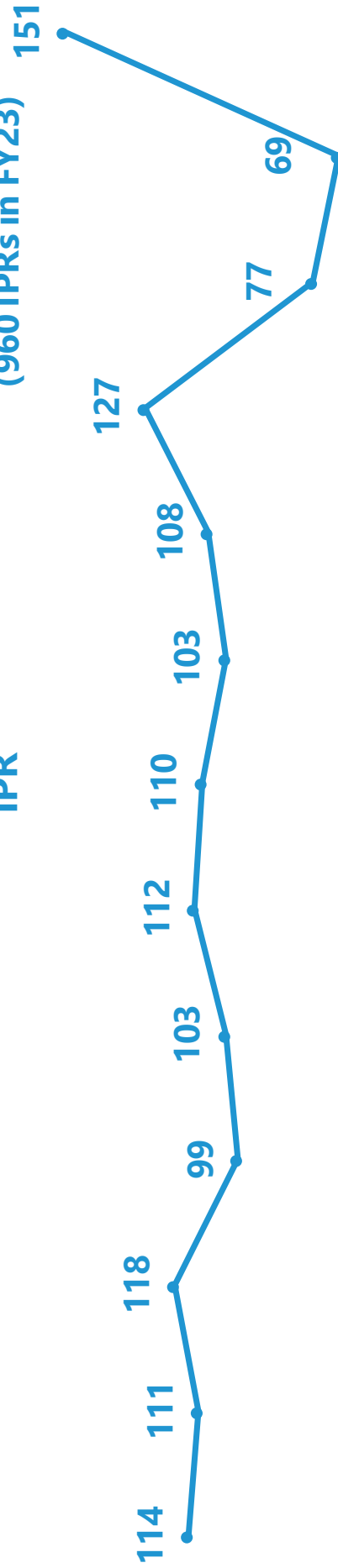
uspto

Petitions filed by month

(June 2023 and Previous 12 Months: Jun. 1, 2022 to Jun. 30, 2023)

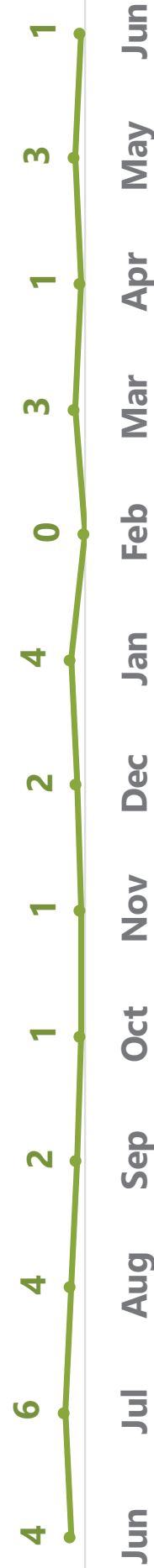
IPR

(960 IPRs in FY23)



PGR

(16 PGRs in FY23)



uspto

Institution rates by petition (FY19 to FY23 through Q3: Oct. 1, 2018 to Jun. 30, 2023)

■ Instituted
■ Denied

by Petition

63%

859

510

FY19

56%

648

512

FY20

58%

702

504

FY21

769

397

FY22

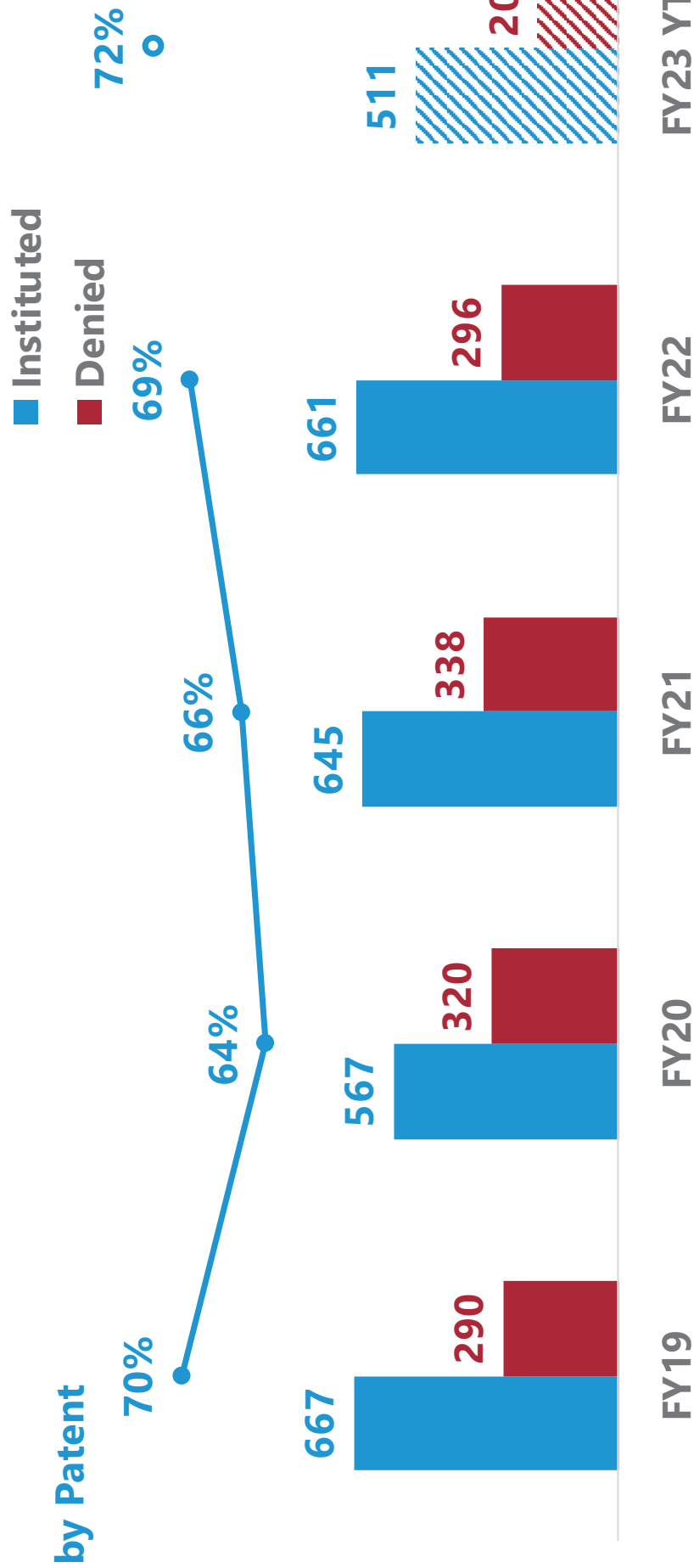
587

288

FY23 YTD

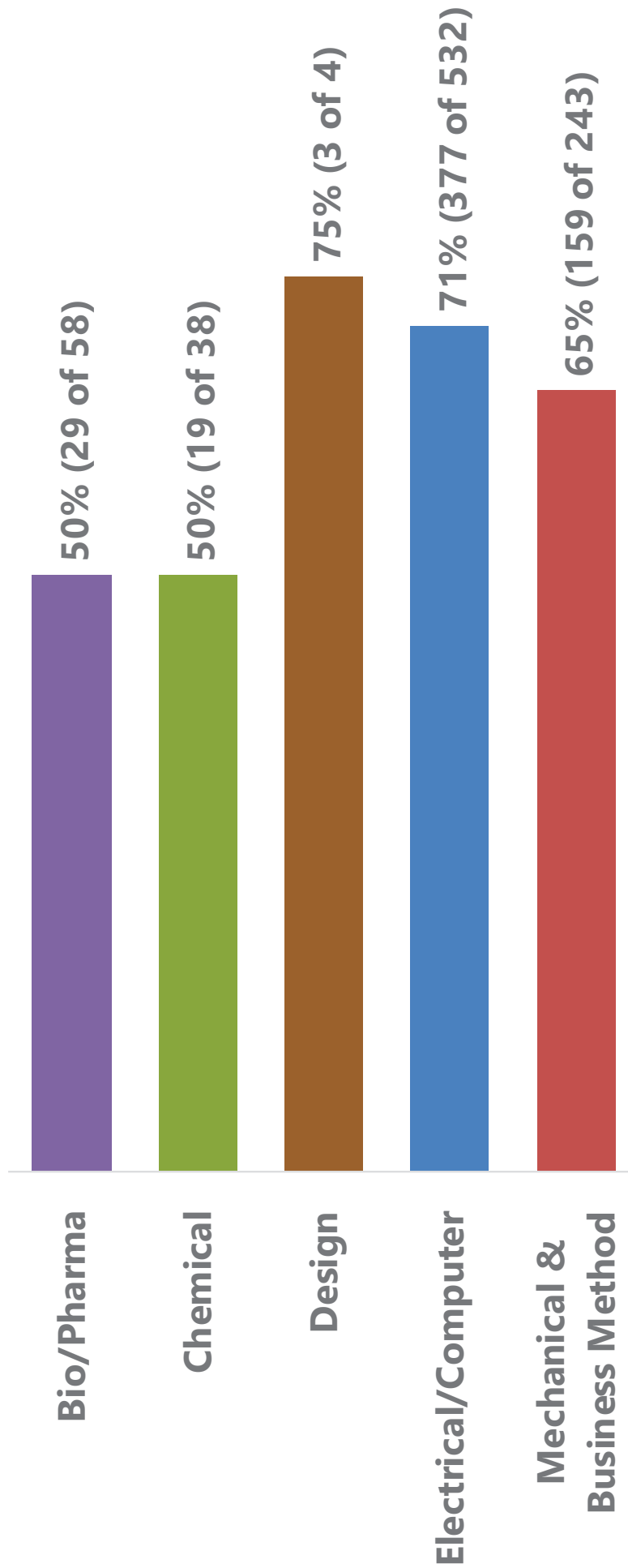
uspto

Institution rates by patent (FY19 to FY23 through Q3: Oct. 1, 2018 to Jun. 30, 2023)



uspto

Institution rates by technology (FY23 through Q3: Oct. 1, 2022 to Jun. 30, 2023)

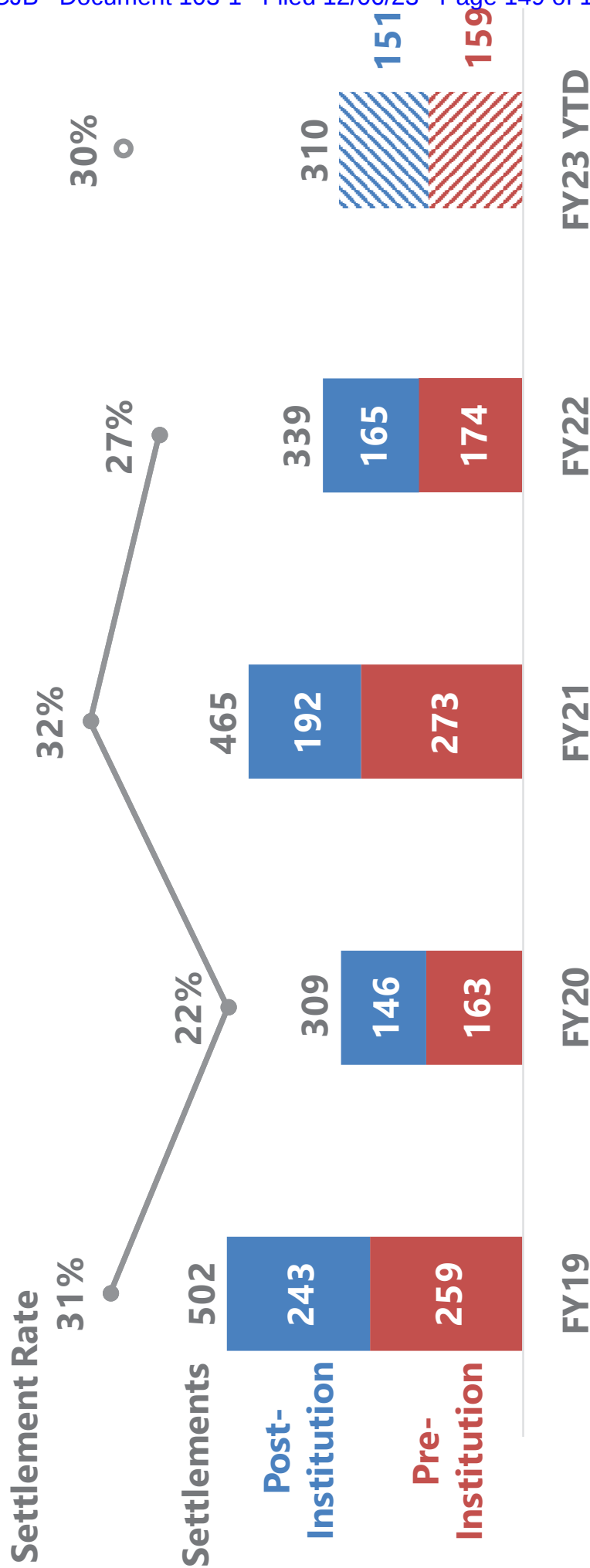


Institution rate for each technology is calculated by dividing petitions instituted by decisions on institution (i.e., petitions instituted plus petitions denied). The outcomes of decisions on institution responsive to requests for rehearing are excluded.

uspto

Settlements

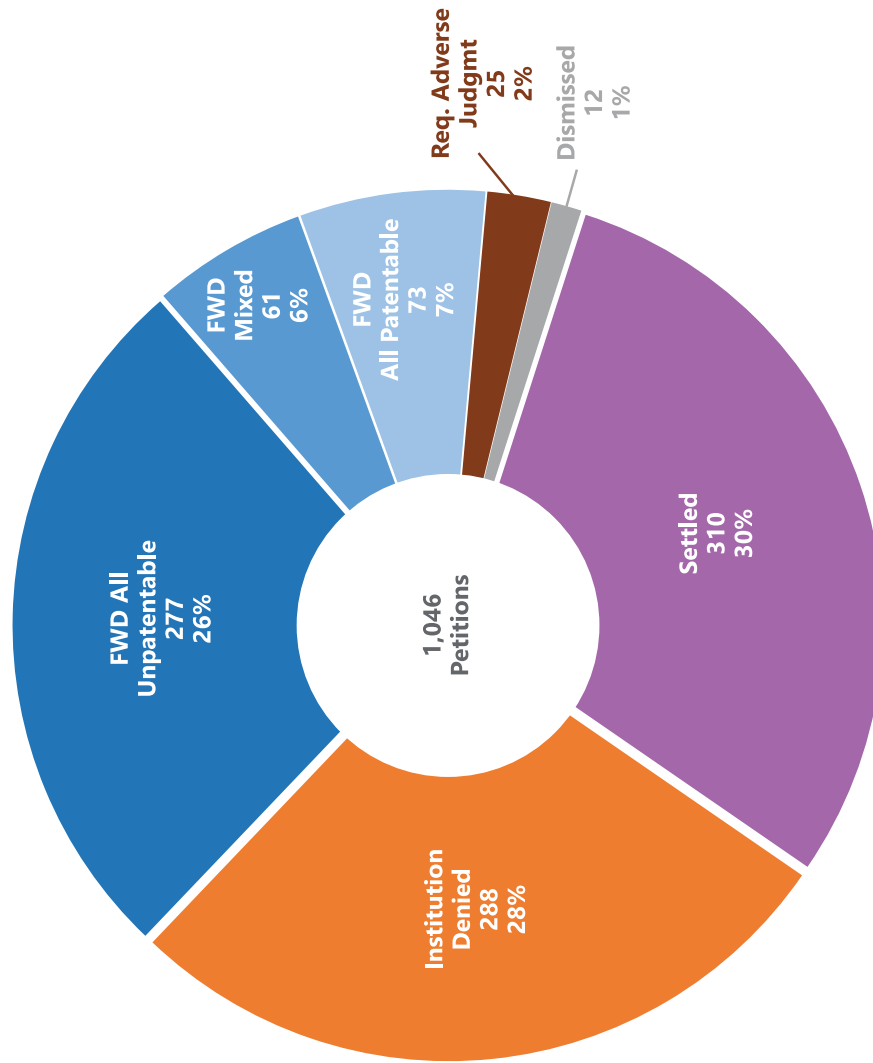
(FY19 to FY23 through Q3: Oct. 1, 2018 to Jun. 30, 2023)



Settlement rate is calculated by dividing total settlements by concluded proceedings in each fiscal year (i.e., denied institution, settled, dismissed, requested adverse judgment, and final written decision), excluding joined cases.



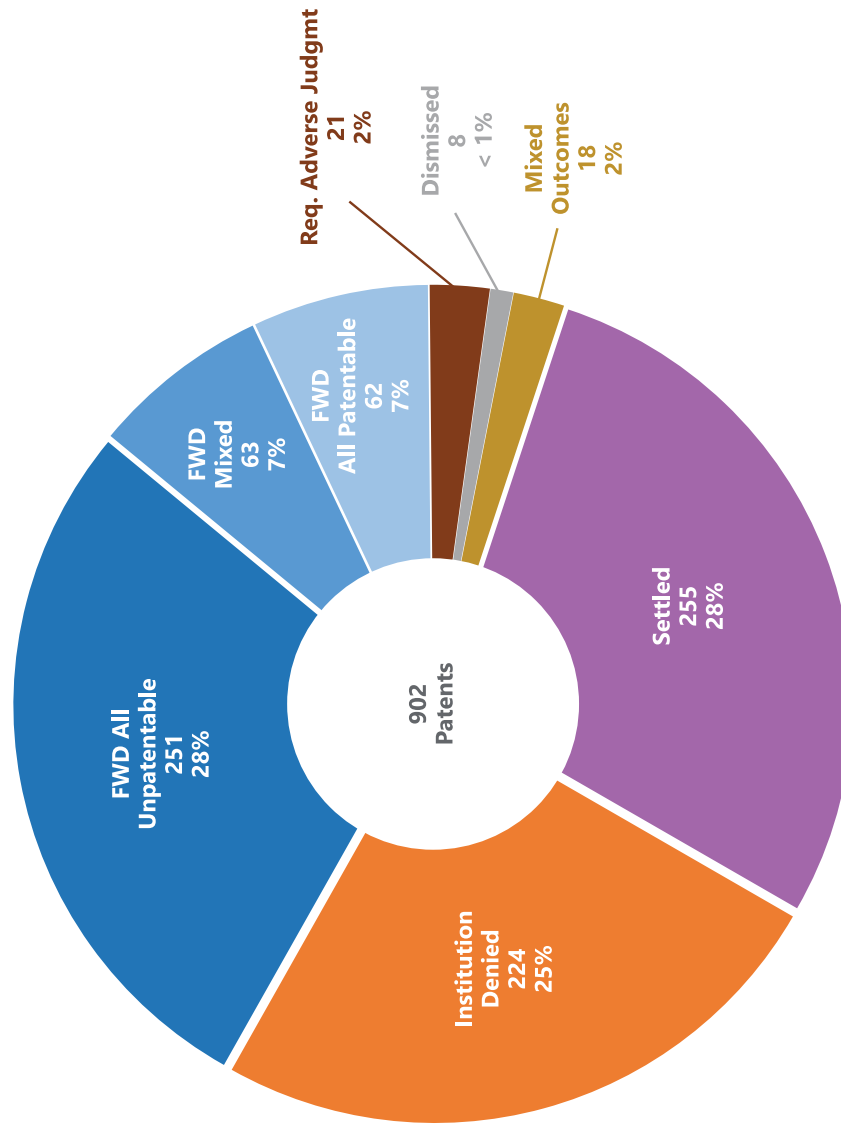
Outcomes by petition (FY23 through Q3: Oct. 1, 2022 to Jun. 30, 2022)



FWD patentability or unpatentability reported with respect to the claims at issue in the FWD. Joined cases are excluded.

uspto

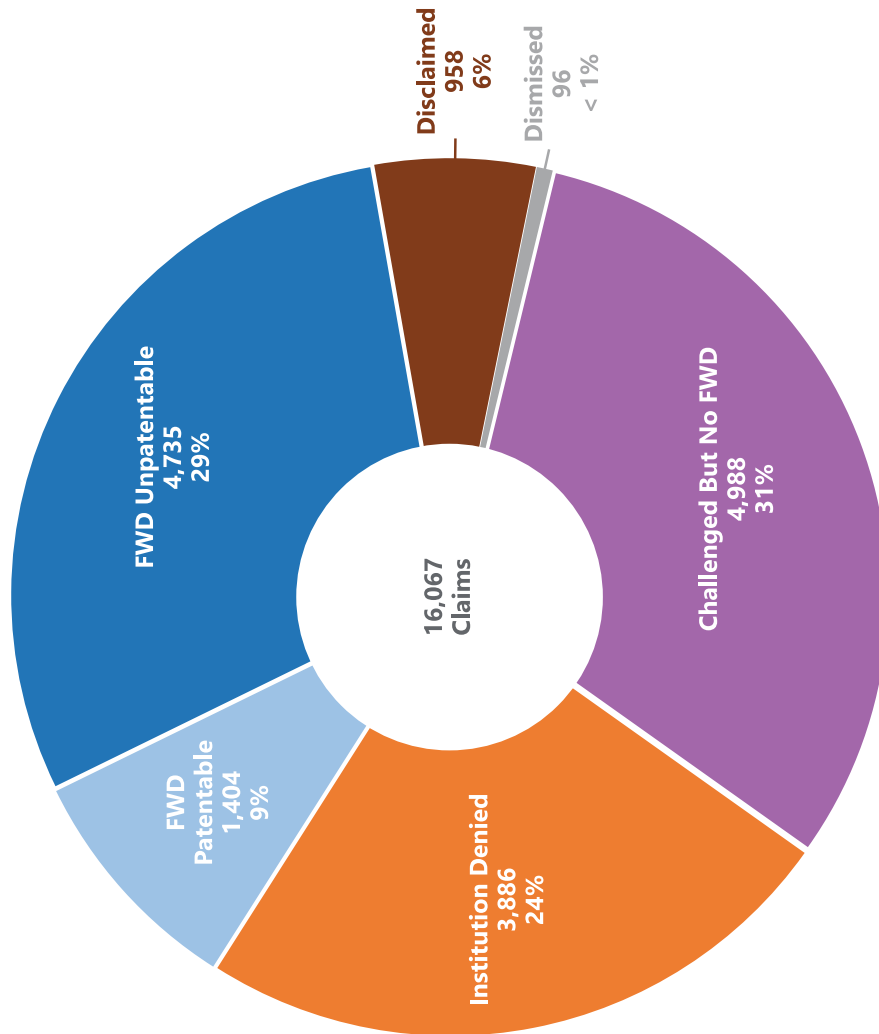
Outcomes by patent (FY23 through Q3: Oct. 1, 2022 to Jun. 30, 2022)



FWD patentability or unpatentability reported with respect to the claims at issue in the FWD. "Mixed Outcome" is shown for patents receiving more than one type of outcome from the list of: denied, settled, dismissed, and/or req. adverse judgement only. A patent is listed in a FWD category if it ever received a FWD, regardless of other outcomes.

uspto

Outcomes by claim challenged (FY23 through Q3: Oct. 1, 2022 to Jun. 30, 2022)



Claim outcomes (FY23 through Q3: Oct. 1, 2022 to Jun. 30, 2022)

